

DOCKET NO.: 257756US6PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Miki MURAKAMI, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP03/16623

INTERNATIONAL FILING DATE: December 24, 2003

FOR: CONTENTS DISTRIBUTION SYSTEM, INFORMATION PROCESSING APPARATUS OR METHOD, AND COMPUTER PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119**  
**AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2003-014245	23 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/16623. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



\_\_\_\_\_  
Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number

22850

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

日本国特許  
JAPAN PATENT OFFICE

PCT/JP03/16023

Rec'd PCT/PTO 15 SEP 2004  
24.12.03

10/507212

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application: 2003年 1月 23日

出願番号  
Application Number: 特願 2003-014245

[ST. 10/C]: [JP 2003-014245]

出願人  
Applicant(s): ソニー株式会社

REC'D 19 FEB 2004

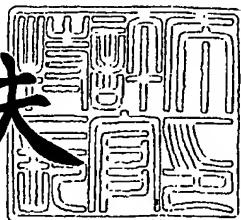
WIPO PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 2月 5日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特 2004-3006560

【書類名】 特許願  
【整理番号】 0290853204  
【提出日】 平成15年 1月23日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 17/00  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 村上 韶  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 久松 史明  
【特許出願人】  
【識別番号】 000002185  
【氏名又は名称】 ソニー株式会社  
【代理人】  
【識別番号】 100093241  
【弁理士】  
【氏名又は名称】 宮田 正昭  
【選任した代理人】  
【識別番号】 100101801  
【弁理士】  
【氏名又は名称】 山田 英治  
【選任した代理人】  
【識別番号】 100086531  
【弁理士】  
【氏名又は名称】 澤田 俊夫

## 【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ配信システム、情報処理装置又は情報処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項 1】

ユーザのクライアントにコンテンツを配信するコンテンツ配信システムであつて、ユーザは2以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

ユーザの各クライアントを登録して顧客関連情報を取得する登録手段と、顧客関連情報を管理する顧客関連情報管理手段と、クライアントからの要求に応じて該要求元クライアントへコンテンツを提供するコンテンツ提供手段と、

前記コンテンツ提供手段からコンテンツを取得したクライアントからの要求に応じて該要求元クライアントへ該取得コンテンツについてのライセンスを提供するライセンス提供手段と、

同一ユーザが持つ1つのクライアントから他のクライアントへのコンテンツの移動が正当であることを示すコンテンツ・コピー証明書を該移動元のクライアントに提供するコンテンツ・コピー証明書提供手段と、を具備することを特徴とするコンテンツ配信システム。

【請求項 2】

前記コンテンツ・コピー証明書提供手段は、移動先のクライアントに対するライセンスを含んだコンテンツ・コピー証明書を生成する、ことを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項 3】

コンテンツ移動元及びコンテンツ移動先の各クライアントはそれぞれ異なるライセンス提供手段に登録され、各ライセンス提供手段は登録クライアントに対して自己の公開鍵を提供し、

前記コンテンツ・コピー証明書提供手段は、コンテンツ移動先のクライアントが登録されているライセンス提供手段の秘密鍵を用いてコンテンツ・コピー証明

書に電子署名を施す、  
ことを特徴とする請求項1に記載のコンテンツ配信システム。

#### 【請求項4】

前記コンテンツ・コピー証明書提供手段は、  
前記コンテンツ移動元のクライアントから移動対象となるコンテンツについて  
のライセンスIDと移動先のクライアントのクライアントIDを取得し、  
前記顧客関連情報関連手段に照会して、移動元のクライアントの正当性、移動  
元のクライアントが移動対象となるコンテンツのライセンスを取得済みであるこ  
と、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実  
際に所持していることを確認してからコンテンツ・コピー証明書を提供する、  
ことを特徴とする請求項1に記載のコンテンツ配信システム。

#### 【請求項5】

前記顧客関連情報管理手段は、リーフIDとクライアントIDの対応テーブル  
、クライアントIDとクライアントの公開鍵証明書の対応テーブル、クライアン  
トIDとユーザIDの対応テーブル、コンテンツIDとライセンスIDの対応テー  
ブル、ユーザIDとダウンロードしたコンテンツのコンテンツIDの対応テー  
ブル、ユーザIDとダウンロードしたライセンスのライセンスIDの対応テー  
ブル、コンテンツ・コピー証明書の発行履歴を管理する、  
ことを特徴とする請求項1に記載のコンテンツ配信システム。

#### 【請求項6】

前記顧客関連情報管理手段は、前記コンテンツ提供手段がクライアントにコン  
テンツを提供し、及び／又は、前記ライセンス提供手段がクライアントにライセ  
ンスを提供する度に顧客関連情報を更新する、  
ことを特徴とする請求項1に記載のコンテンツ配信システム。

#### 【請求項7】

クライアントへのライセンス提供及び／又はコンテンツ・コピー証明書の提供  
に応じてクライアントへの課金処理を行なう課金処理手段をさらに備える、  
ことを特徴とする請求項1に記載のコンテンツ配信システム。

#### 【請求項8】

前記課金処理手段は、ライセンスを提供する場合とコンテンツ・コピー証明書を提供する場合とで差額を設ける、  
ことを特徴とする請求項5に記載のコンテンツ配信システム。

#### 【請求項9】

コンテンツを使用する情報処理装置であって、  
コンテンツをダウンロードするコンテンツ・ダウンロード手段と、  
コンテンツを蓄積するコンテンツ蓄積手段と、  
コンテンツを利用するためのライセンスを取得するライセンス取得手段と、  
取得したライセンスを用いてコンテンツを正当に利用するコンテンツ再生手段と、

コンテンツ移動のためのコンテンツ・コピー証明書を取得するコンテンツ・コピー証明書取得手段と、

前記コンテンツ蓄積手段に蓄積されたコンテンツにコンテンツ・コピー証明書を付加して同一ユーザが所持する他の機器に移動し、又は、コンテンツ・コピー証明書が付加されたコンテンツを同一ユーザが所持する他の機器から取得し、該コンテンツ・コピー証明書の正当性を検証しライセンスを取り出すとともにコンテンツを前記コンテンツ蓄積手段に格納するコンテンツ移動手段と、  
を具備することを特徴とする情報処理装置。

#### 【請求項10】

前記情報処理装置はライセンス・サーバに登録してその公開鍵を受け取り、  
コンテンツ・コピー証明書はライセンス・サーバの秘密鍵で電子署名が施され  
ており、

前記コンテンツ移動手段は、外部から取得したコンテンツ・データに付加され  
ているコンテンツ・コピー証明書の改竄の有無を前記ライセンス・サーバの公開  
鍵を用いてチェックする、  
ことを特徴とする請求項9に記載の情報処理装置。

#### 【請求項11】

コンテンツを使用する情報処理方法であって、  
コンテンツをダウンロードするコンテンツ・ダウンロード・ステップと、

コンテンツを蓄積するコンテンツ蓄積ステップと、  
コンテンツを利用するためのライセンスを取得するライセンス取得ステップと  
、  
取得したライセンスを用いてコンテンツを正当に利用するコンテンツ再生ステップと、  
コンテンツ移動のためのコンテンツ・コピー証明書を取得するコンテンツ・コピー証明書取得ステップと、  
前記コンテンツ蓄積ステップにおいて蓄積されたコンテンツにコンテンツ・コピー証明書を附加して同一ユーザが所持する他の機器に移動し、又は、コンテンツ・コピー証明書が附加されたコンテンツを同一ユーザが所持する他の機器から取得し、該コンテンツ・コピー証明書の正当性を検証しライセンスを取り出すとともにコンテンツを格納するコンテンツ移動ステップと、  
を具備することを特徴とする情報処理方法。

#### 【請求項12】

ライセンス・サーバに登録してその公開鍵を受け取るステップをさらに備え、  
コンテンツ・コピー証明書はライセンス・サーバの秘密鍵で電子署名が施され  
ており、

前記コンテンツ移動ステップでは、外部から取得したコンテンツ・データに付  
加されているコンテンツ・コピー証明書の改竄の有無を前記ライセンス・サーバ  
の公開鍵を用いてチェックする、  
ことを特徴とする請求項11に記載の情報処理方法。

#### 【請求項13】

コンテンツを使用するためのライセンスを提供する処理をコンピュータ・シス  
テム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プロ  
グラムであって、ユーザは2以上のクライアントを所持することができ、各クラ  
イアントはライセンス取得に基づいて正当にコンテンツを利用し、

コンテンツ移動元のクライアントから移動対象となるコンテンツについてのラ  
イセンスIDとコンテンツ移動先のクライアントのクライアントIDを取得する  
ステップと、

コンテンツ移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを判別するステップと、

コンテンツ・コピー証明書を作成するステップと、

コンテンツ・コピー証明書をコンテンツ移動元のクライアントに提供するステップと、

を具備することを特徴とするコンピュータ・プログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などのコンテンツの利用を管理するコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに係り、特に、使用許諾など何らかの契約や利用条件に基づいてコンテンツの利用を管理するコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに関する。

##### 【0002】

さらに詳しくは、本発明は、コンテンツの利用者にライセンスを与えることによりコンテンツの利用を制御しコンテンツの保護を図るコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに係り、特に、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にするコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムに関する。

##### 【0003】

##### 【従来の技術】

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各

種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（xDSL : x Digital Subscriber Line、CATV（Cable TV）、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組みが整いつつある。

#### 【0004】

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起こっている。

#### 【0005】

暗号技術を用いることによって、通信路上に流れるコンテンツを悪意のある第三者から保護することが可能となっている。しかしながら、コンテンツの配信過程だけでなく、コンテンツが正規のユーザに提供された後に行なわれる不正コピーや不正利用も大きな問題となっている。

#### 【0006】

デジタル・コンテンツに関するこの種の問題への対策として、最近では権利管理方式（DRM : Digital Rights Management）と呼ばれる方式が採用されている。以下では、このDRMの概要とその問題点について説明する。

#### 【0007】

##### DRM (Digital Right Management) :

権利情報管理方式（DRM）によって、ユーザはコンテンツの利用許可（ライセンス）を得なければ、コンテンツを利用できない仕組みが実現される。このようなシステムとしては米マイクロソフト社の"Windows Media Right Manager"や、米IBM社の"Electronic Media Management System (EMMS)"と呼ばれるシステムが挙げられる。

#### 【0008】

DRMのシステムは、典型的にはコンテンツ提供者とライセンス管理者とユーザという参加者で構成される。ユーザは、コンテンツの再生装置を所持し、それを使ってコンテンツを利用する。また、ライセンス管理者は、ユーザにライセンスの発行を行なう。また、コンテンツ提供者は、ユーザにコンテンツの提供を行なう。

#### 【0009】

コンテンツ（Cont）は、コンテンツ提供者によって、コンテンツ毎に異なる鍵（コンテンツ鍵 $K_c$ ）で暗号化された形式E（ $K_c$ , Cont）で配布される。本明細書中では、これを「暗号化コンテンツ」と呼ぶことにする。

#### 【0010】

ユーザは、あるコンテンツContを使用する場合、ライセンス管理者に対してライセンス発行を要求する。これに対し、ライセンス発行者は、ユーザへの課金処理などを行なった上でライセンスを発行する。

#### 【0011】

ここで言うライセンスの発行は、実際には、ユーザの再生装置にコンテンツ鍵 $K_c$ を与えることである。このために、ライセンス管理者は再生装置との間で、再生装置毎に異なる暗号鍵 $K_u$ を共有しており（暗号鍵 $K_u$ の共有は、ライセンス発行時に行なわれるか、又はあらかじめ共有したものが再生装置に組み込まれている）、コンテンツ鍵 $K_c$ を暗号鍵 $K_u$ で暗号化したデータE（ $K_u$ ,  $K_c$ ）として再生装置に送付する。このデータのことを「ライセンス・トークン」と呼ぶ。

#### 【0012】

ライセンスを受けたユーザの再生装置は、暗号鍵 $K_u$ と受け取ったライセンス・トークンE（ $K_u$ ,  $K_c$ ）と暗号化コンテンツE（ $K_c$ , Cont）を使って、コンテンツを再生することができる。まず、ライセンス・トークンE（ $K_u$ ,  $K_c$ ）からコンテンツ鍵 $K_c$ を復号し、次いでコンテンツ鍵 $K_c$ を使って暗号化コンテンツE（ $K_c$ , Cont）からコンテンツContを復号して再生する。したがって、再生装置とライセンス・トークンと暗号化コンテンツの組み合わせが正しいときだけ、つまりライセンスを得たユーザだけがコンテンツを利用でき

ることになる。

#### 【0013】

ここで、コンテンツの利用権を保護するためには、再生装置側では、復号されたコンテンツが外部に漏洩することを防がなければならない。このためには、再生装置は、暗号鍵  $K_u$  やコンテンツ鍵  $K_c$  や復号されたコンテンツ  $C_{o n t}$  を外部に漏らさないように処理しなければならない。何故なら、復号されたコンテンツが一旦外部に漏洩すれば、それを複製し利用することが制約なしに可能になるからである。言い換れば、再生装置には、暗号鍵  $K_u$  やコンテンツ鍵  $K_c$ 、並びに復号されたコンテンツ  $C_{o n t}$  を外部に漏らさないで処理できるという条件が必要である。本明細書中では、このような条件を備えた再生装置のことを「正当」とあると呼ぶことにする。

#### 【0014】

DRMでは、コンテンツのライセンス（利用許可）をユーザに与えることは、コンテンツ鍵  $K_c$  をそのユーザの（特定の）再生装置に与えることで実現される。このライセンス供与の際に、コンテンツ鍵  $K_c$  を受け取る再生装置は正当であるという条件が必須である。したがって、ライセンスの発行を行なうライセンス発行者は、発行相手の再生装置を特定し、正当な再生装置だけにコンテンツ鍵を与えるようにしなければならない。このため、ライセンス発行者は正当な再生装置に関するデータベースを持ち、ライセンス発行はそれに基づいて行なう必要がある。

#### 【0015】

しかしながら、多数の再生装置が存在する場合を考えると、このようなデータベースの検索は時間あるいはコストを要する処理となる。特に、コンテンツの毎回ダウンロードなどの仕組みにより、ライセンス発行が頻繁に行なわれる場合、データベースの置かれるサーバの負荷が過剰になる。つまり、DRMでのライセンス発行は、再生装置の個数の増加に対してスケーラビリティのない処理となる。

#### 【0016】

例えば、特定のユーザに対してコンテンツを提供する場合、コンテンツ提供の

前にユーザ認証を行なうことになる。DRMの方法を使うのであれば、さらにユーザ認証に加えてそのユーザが持つコンテンツの再生装置を特定し、再生装置毎にライセンスを生成するという処理が必要になる。このことはコンテンツ提供の処理速度を低下させてしまう。

#### 【0017】

また、ユーザは一般に複数のコンテンツ再生装置を所有し利用するところ、コンテンツのライセンスは特定の再生装置に対して与えることで実現される。このため、ユーザが所有する各再生装置が「正当」である条件を満たしていたとしても、ユーザが同じコンテンツを複数の再生装置に跨って利用したい場合には、個々の再生装置毎にライセンスを得る手続きをとる必要があり、操作が面倒になってしまう。あるいは同じコンテンツを利用するために、逐次課金されてしまうので、過大な対価を強いられることになる。

#### 【0018】

また、コンテンツの流通・配信事業が発展している昨今においては、複数のコンテンツ配信事業者によってさまざまなコンテンツが提供されている。しかしながら、ユーザが所有する各再生装置が「正当」であったとしても、個々の再生装置が異なるコンテンツ配信事業者にライセンス登録していた場合、同じユーザに帰属するにも拘らず、装置間に跨ってコンテンツを利用する（コンテンツを共有する）という融通性がないため、複数のコンテンツ配信事業者に登録した（又はアカウントを取得した）利益を十分に得ることができない。コンテンツ配信事業者側から見れば、事業協力が不十分であり顧客の利便性が低いと言わざるを得ない。

#### 【0019】

##### 【発明が解決しようとする課題】

本発明の目的は、使用許諾など何らかの契約や利用条件に基づいてコンテンツの利用を好適に管理することができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

#### 【0020】

本発明のさらなる目的は、コンテンツの利用者にライセンスを与えることによりコンテンツの利用を制御しコンテンツの保護を好適に図ることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

### 【0021】

本発明のさらなる目的は、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にすることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することにある。

### 【0022】

#### 【課題を解決するための手段及び作用】

本発明は、上記課題を参照してなされたものであり、その第1の側面は、ユーザのクライアントにコンテンツを配信するコンテンツ配信システムであって、ユーザは2以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

ユーザの各クライアントを登録して顧客関連情報を取得する登録手段と、  
顧客関連情報を管理する顧客関連情報管理手段と、  
クライアントからの要求に応じて該要求元クライアントへコンテンツを提供するコンテンツ提供手段と、

前記コンテンツ提供手段からコンテンツを取得したクライアントからの要求に応じて該要求元クライアントへ該取得コンテンツについてのライセンスを提供するライセンス提供手段と、

同一ユーザが持つ1つのクライアントから他のクライアントへのコンテンツの移動が正当であることを示すコンテンツ・コピー証明書を該移動元のクライアントに提供するコンテンツ・コピー証明書提供手段と、  
を具備することを特徴とするコンテンツ配信システムである。

### 【0023】

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する

機能モジュール)が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

#### 【0024】

本発明の第1の側面に係るコンテンツ配信システムによれば、ユーザは、複数のクライアントを所持し、個々のクライアントが異なるライセンス・サーバに登録している場合であっても、1つのクライアント上でダウンロードしたコンテンツを他のクライアントに移動する際、コンテンツの移動先が正当であることを示すコンテンツ・コピー証明書を添付する。そして、移動先のクライアントではコンテンツ・コピー証明書を基に、受け取ったコンテンツを取り込み、再生する権利について正当であることを確認することができる。

#### 【0025】

すなわち、本発明の第1の側面に係るコンテンツ配信システムによれば、コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にすることができる。また、ユーザが複数のクライアント間でコンテンツを利用する作業的な負担が軽減され、コンテンツ配信サービスの利用が促進される。

#### 【0026】

このような複数のクライアント間でのコンテンツの共有は、コンテンツ配信事業者間の協業により実現される。コンテンツの移動元及び移動先となる各クライアントは、それぞれ別個のコンテンツ配信事業者に登録されていてもよい。このような場合、顧客関連情報提供手段によってコンテンツ配信事業者間で互いの顧客関連情報を照会できるようにして、コンテンツ移動元のクライアントを登録する配信事業者は、コンテンツ移動先のクライアントが同じユーザに所持されている正当な機器であることを照合処理するようにすればよい。

#### 【0027】

ここで、前記コンテンツ・コピー証明書提供手段は、移動先のクライアントに対するライセンスを含んだコンテンツ・コピー証明書を生成するようにしてもよい。このような場合、移動先のクライアントは、コンテンツ・コピー証明書からライセンスを取り出してコンテンツを利用することが可能である。したがって、

移動先のクライアント自身は、コンテンツ配信事業者に登録し直接ライセンスを取得するという作業が不要であり、コンテンツの共有を円滑に実現することができる。

#### 【0028】

また、コンテンツ移動元及びコンテンツ移動先の各クライアントはそれぞれ異なるライセンス提供手段に登録され、各ライセンス提供手段は登録クライアントに対して自己の公開鍵を提供するようにしてもよい。このような場合、前記コンテンツ・コピー証明書提供手段は、コンテンツ移動先のクライアントが登録されているライセンス提供手段の秘密鍵を用いてコンテンツ・コピー証明書に電子署名を施すことにより、コンテンツ・コピー証明書の改竄を防止し、安全に移動することができる。また、移動先のクライアントは、その公開鍵を用いて復号し、コンテンツのライセンスを取り出すことができる。

#### 【0029】

また、前記コンテンツ・コピー証明書提供手段は、前記移動元のクライアントから移動対象となるコンテンツについてのライセンスIDと移動先のクライアントのクライアントIDを取得し、さらに前記顧客関連情報関連手段に照会して、移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを確認してからコンテンツ・コピー証明書を提供するようにすることで、コンテンツ・コピー証明書の捏造や悪用を好適に防止することができる。

#### 【0030】

また、前記顧客関連情報提供手段は、リーフIDとクライアントIDの対応テーブル、クライアントIDとクライアントの公開鍵証明書の対応テーブル、クライアントIDとユーザIDの対応テーブル、コンテンツIDとライセンスIDの対応テーブル、ユーザIDとダウンロードしたコンテンツのコンテンツIDの対応テーブル、ユーザIDとダウンロードしたライセンスのライセンスIDの対応テーブル、コンテンツ・コピー証明書の発行履歴を管理すればよい。

#### 【0031】

ここで、前記顧客関連情報管理手段は、前記コンテンツ提供手段がクライアントにコンテンツを提供し、及び／又は、前記ライセンス提供手段がクライアントにライセンスを提供する度に顧客関連情報を更新するようにすればよい。

#### 【0032】

また、本発明の第1の側面に係るコンテンツ配信システムは、クライアントへのライセンス提供に応じてクライアントへの課金処理を行なう課金処理手段をさらに備えていてもよい。

#### 【0033】

そして、前記課金処理手段は、ライセンスを提供する場合とコンテンツ・コピー証明書を提供する場合とで差額を設けるようにてもよい。例えば、同じコンテンツについての2度目のライセンス提供に相当するコンテンツ・コピー証明書の料金を初期のライセンス取得よりも低額にし又は無料にすることにより、ユーザが複数のクライアント間でコンテンツを利用するコスト的な負担が軽減され、コンテンツ配信サービスの利用が促進される。

#### 【0034】

また、本発明の第2の側面は、コンテンツを使用するためのライセンスを提供する処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、ユーザは2以上のクライアントを所持することができ、各クライアントはライセンス取得に基づいて正当にコンテンツを利用し、

コンテンツ移動元のクライアントから移動対象となるコンテンツについてのライセンスIDとコンテンツ移動先のクライアントのクライアントIDを取得するステップと、

コンテンツ移動元のクライアントの正当性、移動元のクライアントが移動対象となるコンテンツのライセンスを取得済みであること、及び、移動元のクライアントを所持するユーザが移動先のクライアントを実際に所持していることを判別するステップと、

コンテンツ・コピー証明書を作成するステップと、

コンテンツ・コピー証明書をコンテンツ移動元のクライアントに提供するステ

ップと、

を具備することを特徴とするコンピュータ・プログラムである。

#### 【0035】

本発明の第2の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第2の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が發揮され、本発明の第1の側面に係るコンテンツ配信システムと同様に、コンテンツの保護を確保しながら複数クライアント間でのコンテンツの共有を実現するという作用効果を得ることができる。

#### 【0036】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

#### 【0037】

##### 【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

#### 【0038】

図1には、本発明の一実施形態に係るコンテンツ配信システムの構成例を模式的に示している。同図に示す例では、コンテンツ配信システムは、コンテンツを提供する配信事業者側と、顧客側に分かれて構成される。配信事業者と顧客の間は、例えばインターネットやその他の広帯域通信網（xDSL : x Digital Subscriber Line、CATV（Cable TV）、無線ネットワークなど）で相互接続されている。

#### 【0039】

コンテンツ配信事業者側は、図示の通り、配信事業者A及びBを始めとして、複数の配信事業者で構成されている。

#### 【0040】

各配信事業者は、顧客のコンテンツ再生装置（以下では、「クライアント」と

呼ぶ) 毎にユーザ(クライアント)登録並びにコンテンツのライセンス供与を行なうライセンス・サーバと、提供すべきコンテンツの蓄積並びに配信処理を行なうコンテンツ・サーバと、ユーザ登録時及び／又はライセンス提供時(並びに、コンテンツ・コピー証明書(後述)発行時)に課金処理を行なう課金サーバと、顧客又はクライアントにコンテンツのライセンスを与えるために必要な各種データを保管する業務系データベース・サーバとを備えている。

#### 【0041】

本実施形態では、各配信事業者間は、例えばインターネットやその他のバックボーン通信網で相互接続されている。また、配信事業者間の事業協力を円滑に行なうために、配信事業者毎の業務系データベースを統括する業務系データベース・サーバC(DB C)が構築されている。

#### 【0042】

各配信事業者毎に設置されている業務系データベース・サーバA(DB A)及び業務系データベース・サーバB(DB B)は、自己に存在しないユーザ情報は業務系DB Cに照会するとともに、更新内容を業務系DB Cに反映させる同期処理を適宜行なうようにする。但し、業務系DB Cは必須ではなく、業務系DB Aと業務系DB Bの間で情報を共有できる何らかの仕組みが備わつていればよい。

#### 【0043】

なお、図1に示す例では、配信事業者A及びBがそれぞれ独自にライセンス・サーバ、課金サーバ、コンテンツ・サーバ、業務系データベース・サーバを構築・保有しているが、一部又は全部のサーバを配信事業者間で共同利用するようにしてもよいし、一方の配信事業者が保有するコンテンツ・サーバを他方の配信事業者が流用するようにしてもよい。

#### 【0044】

コンテンツ配信システム内では多数の顧客が存在するが、図1に示す例では画面の簡素化のため、单一の顧客のみ示している。図示の顧客は、クライアントA並びにクライアントBを始め、複数のコンテンツ再生装置を所有し利用している。各クライアントは、DRMで言う「正当」の条件を備えており、暗号鍵やコン

テンツ鍵、並びに復号されたコンテンツを外部に漏らさないで処理することができる。

#### 【0045】

図示の例では、クライアントAは、配信事業者Aに対して事前登録しており、配信事業者Aからコンテンツの提供並びにライセンスの取得を行なうことができる。また、クライアントBは、配信事業者Bに対して事前登録しており、配信事業所Bからコンテンツの提供並びにライセンスの取得を行なうことができる。

#### 【0046】

クライアントAはライセンス・サーバAに対して事前登録並びにライセンス取得要求を行ない、クライアントBはライセンス・サーバBに対して事前登録並びにライセンス取得要求を行なう。ここで、ライセンス・サーバA及びBは、互いの秘密鍵を所持しているものとする。

#### 【0047】

クライアントAからクライアントBへのコンテンツの移動は、例えばクライアントAでコンテンツ書き込み処理を行なった記録媒体をクライアントBに移動する他、パーソナル・ネットワークを利用してデータ伝送するなどの方法が挙げられる。但し、クライアントAからクライアントBへコンテンツを移動する際、移動元のクライアントAは、コンテンツを配信事業者から既に購入済み（又はライセンス取得済み）であるとする。

#### 【0048】

本実施形態では、ユーザを特定するためにユーザIDを使用するが（後述）、各クライアント固体を特定するクライアントIDを代わりに使用することもできる。また、同一のユーザであっても、配信事業者による各サービスで個別にユーザIDが存在するが、それらのユーザIDが各業務系データベースを利用して関係付け（紐付け）されており、同一のユーザであることを各配信事業者が把握できるものとする。クライアントIDも業務系データベース・サーバA、B、及びCに管理されている。なお、本実施形態では、ユーザIDとパスワードによる認証を行なうようになっているが、クライアントID（機器ID）による認証（機器認証）や、機器認証とユーザ認証の組み合わせによりユーザ情報を取り扱うよ

うにしてもよい。

#### 【0049】

本実施形態に係るコンテンツ配信システムは、以下の事柄を前提条件として備えている。

#### 【0050】

- ①配信されたコンテンツは、配信事業者あるいはコンテンツの著作権を保有する者の意思によって、顧客によるコンテンツ利用範囲を制限することができる（著作権管理されている）環境が提供されている。
- ②この著作権管理環境では、暗号化されたコンテンツと、その暗号を解くライセンスを別物で扱うことができる。
- ③各クライアントが著作権管理・保護を確保するための情報処理方法を備えている（「正当」である）。
- ④それぞれのコンテンツ配信事業者から受信するクライアントは異なる。
- ⑤それぞれのクライアントは、受信したコンテンツをその受信クライアントあるいは受信クライアントに接続可能な記録媒体に保管することができる。
- ⑥各クライアント間においてコンテンツを共有する際、記録媒体や有線・無線通信によって顧客自らがクライアント間でコンテンツのやりとりを行なうことができる。
- ⑦それぞれのコンテンツ配信事業者が有する顧客関連情報（顧客自身の情報、顧客保有クライアントの情報、購入コンテンツの情報など）を交換又は共有することができる。

#### 【0051】

本実施形態に係るコンテンツ配信システムでは、かかる前提条件の下で、クライアントAで取得したコンテンツをクライアントBに保管する際に、クライアントBの情報（クライアントの機器IDなどを含んだ「コンテンツ・コピー証明書（後述）」）をそのコンテンツに付加し、クライアントBを特定できるようにすることにより、コンテンツの保護を担保しながらクライアントA及びB間でのコンテンツの共有を実現することができる。但し、クライアントAは、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。コ

ンテンツを共有するための詳細な処理手順については後述に譲る。

#### 【0052】

図2には、本実施形態に係るコンテンツ配信システムにおいて、各種サーバあるいはクライアントとして動作するホスト装置のハードウェア構成を模式的に示している。

#### 【0053】

メイン・コントローラであるC P U (Central Processing Unit) 101は、オペレーティング・システム（OS）の制御下で、各種のアプリケーションを実行する。本実施形態では、ホストがクライアント端末であればC P U 1 0 1は、配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションを実行する。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、C P U 1 0 1は各種のサーバ・アプリケーションを実行する。図示の通り、C P U 1 0 1は、バス108によって他の機器類（後述）と相互接続されている。

#### 【0054】

主メモリ102は、C P U 1 0 1において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時保管したりするために使用される記憶装置であり、例えばD R A M (Dynamic RAM) のような半導体メモリが使用される。ホストがクライアント端末であればC P U 1 0 1は、配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションが実行プログラムとして主メモリ102にロードされる。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、C P U 1 0 1は各種のサーバ・アプリケーションが実行プログラムとして種メモリ102にロードされる。

#### 【0055】

また、R O M (Read Only Memory) 103は、データを恒久的に格納する半導体メモリであり、例えば、起動時の自己診断テスト（P O S T：Power On Self

Test) や、ハードウェア入出力用のプログラム・コード (BIOS: Basic Input/Output System) などが書き込まれている。

#### 【0056】

ディスプレイ・コントローラ104は、CPU101が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ・コントローラ103において処理された描画データは、例えばフレーム・バッファ（図示しない）に一旦書き込まれた後、ディスプレイ111によって画面出力される。ディスプレイ111の表示画面は、一般に、ユーザからの入力内容やその処理結果（より具体的にはコンテンツの再生画面）、あるいはエラーその他のシステム・メッセージをユーザに視覚的にフィードバックする役割を持つ。

#### 【0057】

入力機器インターフェース105は、キーボード112やマウス113、あるいはその他のユーザ入力機器を対話装置100に接続するための装置である。

#### 【0058】

ネットワーク・インターフェース106は、Ethernet（登録商標）などの所定の通信プロトコルに従って、システム100をLAN（Local Area Network）などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。あるいは、車載端末などの場合には、携帯電話などの無線方式により広域ネットワークに接続するインターフェースであってもよい。

#### 【0059】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信サービスを行なうことができる。

#### 【0060】

例えば、ホストがクライアント端末であれば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションをダウンロードできる他、

コンテンツ配信事業者への事前登録、コンテンツ・サーバからのコンテンツのダウンロード、ライセンス・サーバからのコンテンツのライセンス取得、ライセンス取得に伴う課金処理などの手続きをネットワーク経由でダウンロードすることができる。また、コンパイル前のソース・プログラムやコンパイル処理後のオブジェクト・プログラムなどを、ネットワーク経由で実行することができる。また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、各種のサーバ・アプリケーションをネットワーク経由でダウンロードできる他、顧客のクライアント端末との事前登録、コンテンツ配信、ライセンス提供、ライセンス提供に伴う課金処理などの手続きをネットワーク経由で実行することができる。

#### 【0061】

外部機器インターフェース107は、ハード・ディスク・ドライブ（HDD）114やメディア・ドライブ115などの外部装置をホスト100に接続するための装置である。

#### 【0062】

HDD114は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でHDD114上に置くことを、プログラムのシステムへの「インストール」と呼ぶ。通常、HDD114には、CPU101が実行すべきオペレーティング・システムのプログラム・コードや、アプリケーション・プログラム、デバイス・ドライバなどが不揮発的に格納されている。

#### 【0063】

例えば、ホストがクライアント端末であれば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションなどを、HDD114上にインストールすることができる。また、コンテンツ配信事業者からダウンロードした（又は他のクライアント端末から記録媒体などを介して移動された）コンテンツやコンテンツのライセンスなどをHDD114上に蓄積することができる。

また、ホストが、ライセンス・サーバ、コンテンツ・サーバ、課金サーバ、業務系データベース・サーバなどのサーバとして動作する場合には、各種のサーバ・アプリケーションをHDD114上にインストールすることができる他、コンテンツ配信業務に必要な顧客関連情報（顧客自体の情報、顧客保有クライアントの情報、購入コンテンツの情報など）をHDD114上に蓄積することができる。

#### 【0064】

メディア・ドライブ115は、CD（Compact Disc）やMO（Magneto-Optical disc）、DVD（Digital Versatile Disc）などの可搬型メディアを装填して、そのデータ記録面にアクセスするための装置である。

#### 【0065】

可搬型メディアは、主として、ソフトウェア・プログラムやデータ・ファイルなどをコンピュータ可読形式のデータとしてバックアップすることや、これらをシステム間で移動（すなわち販売・流通・配布を含む）する目的で使用される。例えば、コンテンツ配信事業者への事前登録、コンテンツのダウンロード、ライセンス取得、コンテンツの保管などの業務サービスを行なうクライアント・アプリケーションや各種のサーバ・アプリケーションなどを、これら可搬型メディアを利用して複数の機器間で物理的に流通・配布することができる。また、コンテンツ配信事業者からダウンロードしたコンテンツをクライアント端末間で移動するために可搬型メディアを利用することができる。また、コンテンツ配信業務に必要な顧客関連情報（顧客自体の情報、顧客保有クライアントの情報、購入コンテンツの情報など）を配信事業者間で交換又は共有するために可搬型メディアを利用することができる。

#### 【0066】

図3には、ホストがクライアントとして動作するときの機能構成を模式的に示している。同図に示すように、クライアントは、事前登録部と、コンテンツ・ダウンロード部と、コンテンツ蓄積部と、コンテンツ移動処理部と、ライセンス取得・管理部と、課金処理部と、コンテンツ再生処理部で構成される。図示の各機能モジュールは、実際にはCPU101が所定のプログラム・モジュールを実行するという形態で実現される。

**【0067】**

事前登録部は、クライアント上で特定の配信事業者からコンテンツの提供を受けそのライセンスを取得する前提として、ライセンス・サーバとの間で事前登録処理を行なう。事前登録処理の詳細については後述に譲る。

**【0068】**

コンテンツ・ダウンロード部は、事前登録を行なった配信事業者のコンテンツ・サーバから所望のコンテンツをダウンロードする処理を行なう。通常、ユーザはクライアントのブラウザ画面を介してコンテンツを選択した後、コンテンツのダウンロードが起動されるが、このような処理事態は周知なので、本明細書ではこれ以上説明しない。ダウンロードされたコンテンツは、コンテンツ蓄積部に格納される。

**【0069】**

ライセンス取得・管理部は、コンテンツ・サーバからダウンロードしたコンテンツ、あるいはコンテンツ移動処理部を介して同一ユーザの他のクライアントから取得したコンテンツを利用するためには必要なライセンスをライセンス・サーバから取得するとともに、取得したライセンス並びに事前登録時に取得した情報を管理する。

**【0070】**

また、取得したライセンスの有効期限が既に切れている場合には、ライセンス取得・管理部は、ライセンス・サーバに対するライセンス更新処理を行なう。ライセンス取得処理並びにライセンス更新処理の詳細については、後述に譲る。

**【0071】**

また、ダウンロードしたコンテンツを同一ユーザの別クライアントに移動（コピー）する場合には、ライセンス取得・管理部は、ライセンス・サーバに対してコンテンツ・コピー証明書の取得を行なう。また、一旦取り込んだコンテンツ・コピー証明書の通し番号を、「使用済みコンテンツ・コピー証明書」として記録する。コンテンツ・コピー証明書の取得処理の詳細については、後述に譲る。

**【0072】**

また、ライセンス取得・管理部は、別クライアントからコンテンツ・コピー証

明書付きでコンテンツをコピーした際に、このコンテンツ・コピー証明書の中から取り出されたライセンスを保管する。

#### 【0073】

課金処理部は、配信時業者側の課金サーバに接続し、コンテンツ・サーバからダウンロードしたコンテンツ、あるいはコンテンツ移動処理部を介して同一ユーザの他のクライアントから取得したコンテンツを利用（コンテンツ再生）するためのライセンスを取得した対価、並びにコンテンツ・コピー証明書を取得した対価の支払い処理を実行する。

#### 【0074】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信時業者側に委ねられ、課金サーバによって制御される。

#### 【0075】

コンテンツ再生処理部は、コンテンツ蓄積部から所望のコンテンツを取り出し、ライセンス取得・管理部に保管されている（又はコンテンツ・コピー証明書から取り出された）ライセンスを利用して、暗号化されているコンテンツ・データを復号並びにデコードし、その再生処理を行なう。コンテンツの再生処理は、音楽データを音響出力したり、映像データをディスプレイから表示出力したりすることを指す。

#### 【0076】

コンテンツ移動処理部は、同一ユーザ内の他のクライアントとの間でコンテンツの移動を行なう。他のクライアントへコンテンツを移動する場合には、コンテンツ移動処理部は、コンテンツ蓄積部から移動の対象となるコンテンツを取り出し、ライセンス・サーバから取得したコンテンツ・コピー証明書を付加して、可搬型の記録媒体に書き込んだり、あるいは有線・無線の通信路を経由して転送したりする。

#### 【0077】

また逆に、他のクライアントから移動したコンテンツを取り込む場合には、装

填された記録媒体からコンテンツを読み込んだり、有線・無線の通信路を経由してコンテンツを受信したりする。移動されたコンテンツはコンテンツ蓄積部に格納される。このとき、コンテンツ移動処理部は、コンテンツに付加されているコンテンツ・コピー証明書からライセンスを取り出し、これをライセンス取得・管理部に保管する。

#### 【0078】

図4には、ホストがライセンス・サーバとして動作するときの機能構成を模式的に示している。同図に示すように、ライセンス・サーバは、事前登録部と、ライセンス発行部と、ライセンス蓄積部と、データベース管理部とで構成される。図示の各機能モジュールは、実際にはCPU101が所定のプログラム・モジュールを実行するという形態で実現される。

#### 【0079】

事前登録部は、クライアントが当該配信事業者によるコンテンツ配信サービスを利用する前提として、クライアントの事前登録処理を行なう。事前登録処理の詳細については後述に譲る。

#### 【0080】

ライセンス蓄積部は、配信事業者が提供する各コンテンツに必要なライセンスを蓄積している。各ライセンスは、ライセンスIDなどのライセンス指定情報をを利用して検索することができる。

#### 【0081】

ライセンス発行部は、クライアントが、ダウンロードしたコンテンツを利用する際に必要となるライセンスをライセンス蓄積部から取り出して、要求元のクライアントへ送信する。ライセンス発行部は、ライセンスの発行に伴い、クライアントへ課金を行なうため、課金サーバに通知する。ライセンス発行部は、ライセンスにリーフIDを付加する機能（ライセンス蓄積部より取り出したライセンスを加工する機能）も備えている。

#### 【0082】

また、ライセンス発行部は、ユーザがあるクライアントから別クライアントへコンテンツを移動する際に、コンテンツの移動が正当であることを証明するため

のコンテンツ・コピー証明書を発行し、コンテンツ移動元のクライアントへ送信する。ライセンス発行部は、コンテンツ・コピー証明書の発行に伴い、クライアントへ課金を行なうため、課金サーバに通知する。

#### 【0083】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信事業者側に委ねられ、課金サーバによって制御される。

#### 【0084】

また、ライセンス発行部は、クライアント側からの有効期限の切れたライセンスの更新要求に応答して、ライセンスの更新処理も行なう。ライセンスの更新処理の詳細については後述に譲る。

#### 【0085】

データベース管理部は、事前登録部における事前登録の内容や、ライセンス発行部において発行したライセンス情報を業務系データベースへ登録・更新処理する。

#### 【0086】

図5には、ホストがコンテンツ・サーバとして動作するときの機能構成を模式的に示している。同図に示すように、コンテンツ・サーバは、送受信部と、配信コンテンツ蓄積部と、コンテンツ取出部と、暗号化部と、で構成される。図示の各機能モジュールは、実際にはCPU101が所定のプログラム・モジュールを実行するという形態で実現される。

#### 【0087】

送受信部は、クライアントからのコンテンツ要求（コンテンツの指定情報）を受信したり、指定されたコンテンツ・データを要求元クライアントに送信したりする処理を行なう。

#### 【0088】

配信コンテンツ蓄積部は、配信事業者において配信サービスを行なっているコンテンツ・データを保存・管理している。本実施形態では、コンテンツ・データ

は A T R A C (Adaptive Transform Acoustic Coding) 3 方式でエンコードされた状態で配信コンテンツ蓄積部に格納されている。

#### 【0089】

コンテンツ取出部は、送受信部で受信したコンテンツの指定情報を解析して、指定されたコンテンツを配信コンテンツ蓄積部から取り出して、暗号化部へ渡すようになっている。

#### 【0090】

暗号化部は、クライアントへ配信するコンテンツを、コンテンツ・キー  $K_c$  を用いて暗号化する。

#### 【0091】

データベース管理部は、クライアントに対してコンテンツの配信サービスを行なった情報を業務系データベースへ登録・更新処理する。

#### 【0092】

コンテンツの共有処理の前に、クライアント A 及び B は、それぞれライセンス・サーバ A 及び B にアクセスして事前登録処理を行なう。この事前登録処理を行なうことで、リーフ ID、DNK (デバイス・ノード・キー)、各クライアントの秘密鍵及び公開鍵のペア、ライセンス・サーバの公開鍵、及び各公開鍵の証明書を含む「サービス・データ」を取得しておく。

#### 【0093】

ここで、リーフ ID は、クライアント毎に割り当てられた識別情報を表わし、DNK は、そのライセンスに対応する EKB (有効化ブロック) に含まれる暗号化されているコンテンツ・キー  $K_c$  を復号するのに必要なデバイス・ノード・キーである。なお、DNK については、本出願人に既に譲渡されている WO 02 / 080446 号明細書に記述されているが、その詳細な仕組み自体は本発明の要旨に直接関連しないので、本明細書中では説明を省略する。

#### 【0094】

図 6 には、クライアントがライセンス・サーバに事前登録を行なうための処理手順をフローチャートの形式で示している。

#### 【0095】

クライアントは、自己の登録先となるコンテンツ配信事業者のライセンス・サーバに対して、サービス・データ要求を送信する（ステップS1）。

#### 【0096】

ライセンス・サーバは、クライアントからサービス・データ要求を受信すると、これに応答して、要求元クライアントにユーザ情報要求を送信する（ステップS11）。

#### 【0097】

クライアントは、ユーザ情報要求を受信すると、ディスプレイなどにユーザ情報の入力を促すメッセージ並びにユーザ情報の入力画面を表示する（ステップS2）。そして、ユーザがキーボードやマウスなどの入力装置を介して、ユーザの個人情報や決済情報などのユーザ情報を入力すると、これをライセンス・サーバに送信する（ステップS3）。（本実施形態では、ユーザIDとパスワードによる認証を行なうようになっているが、クライアントID（機器ID）による認証（機器認証）や、機器認証とユーザ認証の組み合わせによりユーザ情報を取り扱うようにしてもよい。）

#### 【0098】

ライセンス・サーバは、ユーザ情報を受信すると、そのライセンス・サーバに割り当てられたカテゴリのノード以下のリーフのうち、未だ割り当てられていないリーフを要求元クライアントに割り当て、そのリーフからライセンス・サーバに割り当てられたカテゴリのノードまでのパス上のノードに割り当てられたノード・キーの組をデバイス・ノード・キーDNKとして生成する。そして、生成されたDNKと、クライアントに割り当たされたリーフのリーフIDと、クライアントの秘密鍵及び公開鍵のペアと、ライセンス・サーバの公開鍵及び公開鍵の証明書を含むサービス・データを生成する（ステップS12）。そして、要求元クライアントに対して、このサービス・データを送信する（ステップS13）。

#### 【0099】

また、ライセンス・サーバは、サービス・データの送信後、ユーザ情報をリーフIDに対応付けて記録しておくとともに、事前登録の内容を業務系データベースに登録する（ステップS14）。

**【0100】**

クライアントは、ライセンス・サーバからサービス・データを受信すると、これを暗号化して、ライセンス取得・管理部において保管しておく（ステップS4）。

**【0101】**

以上のようにして、ライセンス・サーバはクライアント及びユーザを登録し、クライアントは所望のコンテンツ配信サービスを利用するためには必要なデバイス・ノード・キーを含むサービス・データを受け取ることができる。

**【0102】**

本実施形態では、各配信事業者の業務系データベース・サーバA及びBは、顧客関連情報を管理するために、以下に示すような複数のテーブルを保有しており、コンテンツ・サーバなどの他のサブシステムは必要に応じてこれらのテーブルを利用（参照、追記、書き換えなど）することができる。

**【0103】**

- (1) リーフIDとクライアントIDの対応テーブル
- (2) クライアントIDとクライアントの公開鍵証明書の対応テーブル
- (3) クライアントIDとユーザIDの対応テーブル
- (4) ユーザIDとユーザ・パスワードの対応テーブル
- (5) コンテンツIDとライセンスIDの対応テーブル
- (6) ユーザIDとダウンロードしたコンテンツのコンテンツIDの対応テーブル（他にダウンロードした日時やライセンスIDなども記録することができる）
- (7) ユーザIDとダウンロードしたライセンスのライセンスIDの対応テーブル（他にダウンロードした日時なども記録することができる）
- (8) コンテンツ・コピー証明書の発行履歴

**【0104】**

また、業務系データベース・サーバCは、上記の業務系データベース・サーバA及びBに保管されている顧客関連情報のうち以下に示す情報を、配信事業者間で共有するために設置されており、双方の配信事業者A及びBは必要なときにその内容を参照したり更新したりすることができる。

**【0105】**

- (1) リーフ I Dとクライアント I Dの対応テーブル
- (2) クライアント I Dとクライアントの公開鍵証明書の対応テーブル
- (3) クライアント I Dとユーザ I Dの対応テーブル
- (4) コンテンツ I Dとライセンス I Dの対応テーブル
- (5) ユーザ I Dとダウンロードしたコンテンツのコンテンツ I Dの対応テーブル（他にダウンロードした日時やライセンス I Dなども記録することができる）
- (6) ユーザ I Dとダウンロードしたライセンスのライセンス I Dの対応テーブル（他にダウンロードした日時なども記録することができる）

**【0106】**

本実施形態に係るコンテンツ配信システムでは、クライアント Aで取得したコンテンツをクライアント Bに保管する際に、「コンテンツ・コピー証明書」をそのコンテンツに付加し、クライアント Bを特定できるようにすることにより、コンテンツの保護を担保しながらクライアント A及びB間でのコンテンツの共有を実現することができる。

**【0107】**

このコンテンツの共有は、図1に示すように以下の手順 P 1～P 6 に従って行なわれる。但し、クライアント Aは、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。また、ライセンス・サーバA及びBは互いの秘密鍵をあらかじめ記憶している。また、各クライアントのクライアント I Dがユーザ I Dと対応付けて、業務系データベースに記録されている。

**【0108】**

- P 1：コンテンツのダウンロード
- P 2：ライセンスのダウンロードとコンテンツの再生
- P 3：業務系データベース間の情報更新
- P 4：コンテンツ・コピー証明書の発行
- P 5：コンテンツ及びコンテンツ・コピー証明書の記録媒体へのコピー
- P 6：コンテンツ取り込み処理

**【0109】**

以下、各段階に手順について説明する。

#### 【0110】

##### コンテンツのダウンロード：

図7には、コンテンツをダウンロードする際のクライアントA側の処理手順をフローチャートの形式で示している。

#### 【0111】

ユーザがディスプレイ画面をキーボードやマウスなどの入力装置を介して操作することによって、コンテンツのダウンロード処理が起動される。これに応答して、ネットワーク・インターフェース106を介して、コンテンツ・サーバAへアクセスする（ステップS21）。

#### 【0112】

コンテンツ・サーバAへアクセスした結果、クライアントのディスプレイ画面上には、コンテンツ選択画面（図示しない）が表示される。ユーザは、同画面上で、キーボードやマウスなどの入力装置を介して所望のコンテンツを指定する。そして、クライアントAはコンテンツを指定する情報をコンテンツ・サーバAへ通知する（ステップS22）。さらに、コンテンツ・サーバAに対してユーザIDを通知する（ステップS23）。

#### 【0113】

後述するように、コンテンツ・サーバAは、コンテンツ指定情報の通知に応答して、該当するコンテンツを暗号化して送信してくれる。クライアントAは、暗号化コンテンツを受信して（ステップS24）、これをコンテンツ蓄積部に格納する（ステップS25）。

#### 【0114】

また、図8には、コンテンツをダウンロードする際のコンテンツ・サーバ側の処理手順をフローチャートの形式で示している。

#### 【0115】

コンテンツ・サーバAは、クライアントAよりアクセスを受けるまで待機する（ステップS31）。そして、アクセスを受けたと判断すると、クライアントAから送信されてきた、コンテンツを指定する情報を取り込む（ステップS32）

。このコンテンツを指定する情報は、図6に示したフローチャートのステップS22において、クライアントAが通知してきた情報に該当する。

#### 【0116】

次いで、コンテンツ・サーバAは、蓄積しているコンテンツの中から、先行ステップS32において取り込まれた情報で指定されたコンテンツを読み出す（ステップS33）。

#### 【0117】

そして、読み出されたコンテンツを、コンテンツ・キーKcを用いて暗号化する（ステップS34）。配信コンテンツ蓄積部に記憶されている・コンテンツ・データは、既にATRAC3方式によりエンコードされているので、このエンコードされたコンテンツ・データが暗号化されることになる。なお、コンテンツ・データをあらかじめ暗号化してから配信コンテンツ蓄積部に格納しておくことにより、ステップS34を省略することができる。

#### 【0118】

次いで、業務系データベースAから、コンテンツIDに対応したライセンスIDを取り込む（ステップS35）。そして、暗号化したコンテンツ・データを伝送するフォーマットを構成するヘッダに、暗号化コンテンツを復号するのに必要なキー情報（後述）と、コンテンツを利用するのに必要なライセンスを識別するライセンスIDを付加する（ステップS36）。

#### 【0119】

そして、ステップS34において暗号化したコンテンツと、ステップS36においてキーとライセンスIDを付加したヘッダとをフォーマット化したデータを、要求元のクライアントAに送信する（ステップS37）。

#### 【0120】

最後に、クライアントAのユーザIDと送信したコンテンツのコンテンツIDを業務系データベースAに記録する（ステップS38）。業務系データベースAに記録した内容は、同期処理により業務系データベースCにも反映されており、他方の配信事業者Bからも利用することができる。

#### 【0121】

図9には、コンテンツ・サーバAからクライアントAにコンテンツを配信するときに用いられるデータ・フォーマットの構成例を示している。同図に示すように、このフォーマットは、ヘッダ（Header）とデータ（Data）とで構成される。

#### 【0122】

ヘッダには、コンテンツ情報（Content Information）と、ライセンスID（License ID）と、イネーブリング・キー・ブロック（有効化キー・ブロック：E KB（Enabling Key Block））と、E KBから生成されたキーK<sub>EKB</sub>を用いて暗号化されたコンテンツ・キーK<sub>c</sub>としてのデータK<sub>EKB</sub>（K<sub>c</sub>）が配置されている。なお、E KBに関しては、本出願人に既に譲渡されているWO 02/080446に記載されているが、本発明の要旨には直接関連しないので、本明細書中では説明を省略する。

#### 【0123】

コンテンツ情報には、データとしてフォーマット化されているコンテンツ・データを識別するための識別情報としてのコンテンツID（C ID）と、そのコンテンツのコーデックの方式などの情報が含まれている。

#### 【0124】

データは、任意の数の暗号化ブロック（Encryption Block）により構成される。各暗号化ブロックは、イニシャル・ベクトル（I V：Initial Vector）と、シード（S e e d）と、コンテンツ・データをキーK'<sub>c</sub>で暗号化したデータE<sub>K'</sub><sub>c</sub>（Data）とで構成される。

#### 【0125】

キーK'<sub>c</sub>は、以下の式により示されるように、コンテンツ・キーK<sub>c</sub>と、乱数で設定されるシードにハッシュ関数を適用して演算された値で構成される。

#### 【0126】

##### 【数1】

$$K'c = \text{Hash}(K_c, \text{Seed})$$

#### 【0127】

イニシャル・ベクトルI VとシードS e e dは、各暗号化ブロック毎に異なる

値に設定される。

#### 【0128】

この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行なわれる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行なわれるCBC(Cipher Block Chaining)モードで行なわれる。

#### 【0129】

CBCモードの場合、最初の8バイトのコンテンツ・データを暗号化するとき、その前段の8バイトの暗号化の結果が存在しないため、最初の8バイトのコンテンツ・データを暗号化するときはイニシャル・ベクトルIVを初期値として暗号化が行なわれる。

#### 【0130】

このCBCモードによる暗号化を行なうことで、1つの暗号化ブロックが解読されたとしても、その影響が他の暗号化ブロックに及ぶことが抑制される。なお、この暗号化の処理手順に関しては本出願人に既に譲渡されているWO 02/080446に記載されているが、本発明の要旨には直接関連ないので、本明細書中ではこれ以上説明しない。また、暗号化方式については、これに限らず、単にコンテンツ・キー $K_c$ でコンテンツ・データを暗号化するように構成してもよい。

#### 【0131】

以上のようにして、クライアントAは、コンテンツ・サーバAからコンテンツを自由に取得することができる。コンテンツを利用(再生)するためにはコンテンツのライセンスを別途取得する必要があることから、本実施形態では、コンテンツの配信自体は無料とし、ライセンスの取得を有料にしている。したがって、コンテンツそのものは無料で、大量に配布することが可能である。

#### 【0132】

##### ライセンスのダウンロードとコンテンツの再生：

図10には、クライアントA側でダウンロードしたコンテンツを再生するための処理手順をフローチャートの形式で示している。

#### 【0133】

まず、クライアントAは、ユーザがキーボードやマウスなどの入力装置の操作を介して指示したコンテンツの識別情報（C I D）を取得する（ステップS 4 1）。この識別情報は、例えば、コンテンツのタイトルや、記憶されているコンテンツ毎に付与されている番号などで構成される。

#### 【0134】

コンテンツが指示されると、次いで、そのコンテンツに対応するライセンスID（そのコンテンツを使用するのに必要なライセンスの識別情報）を読み取る。このライセンスIDは、図9に示したように、暗号化されているコンテンツ・データのヘッダに記述されている。

#### 【0135】

次いで、読み取られたライセンスIDに対応するライセンスが、クライアントにより既に取得され、ライセンス取得・管理部に保管されているかどうかを判断する（ステップS 4 2）。ここで、該当するライセンスが未だ取得されていない場合には、ステップS 4 3に進み、ライセンス取得処理（後述）を実行する。

#### 【0136】

ステップS 4 2において、ライセンスが既に取得されていると判断された場合、あるいはステップS 4 3においてライセンス取得処理が実行された結果、ライセンスが取得された場合、さらに、取得されているライセンスが有効期限内かどうかを判断する（ステップS 4 4）。ライセンスが有効期限内のものであるかどうかは、ライセンスの内容として規定されている期限（後述）と、クライアントのシステム・タイマにより計時されている現在日時と比較することで判断される。

#### 【0137】

ライセンスの有効期限が既に満了していると判断された場合には、ステップS 4 5に進み、ライセンスの更新処理（後述）を実行する。

#### 【0138】

ステップS 4 4において、ライセンスが有効期限内であると判断された場合、あるいはステップS 4 5においてライセンスが更新された場合、さらにライセンスが正当であるかどうかを判断する（ステップS 4 6）。ライセンスの有効性は

、ライセンスに含まれている電子署名（後述）を利用して実行することができる。ライセンスが正当でない場合には、エラー処理を行なってから（ステップS47）、本処理ルーチン全体を終了する。エラー処理は、正当なライセンスを改めて取得する処理であってもよい。

#### 【0139】

ステップS46において、ライセンスが正当であると判断された場合、該当する暗号化コンテンツ・データをコンテンツ蓄積部から読み出す（ステップS48）。そして、暗号化されているコンテンツ・データを、図9に示したデータに配置されている暗号化ブロック単位で、コンテンツ・キー $K_c$ を用いて復号する（ステップS49）。

#### 【0140】

さらに、復号されたコンテンツ・データをデコードし、コンテンツの再生処理を行なう（ステップS50）。コンテンツの再生処理は、音楽データを音響出力したり、映像データをディスプレイから表示出力したりすることを指す。

#### 【0141】

図11には、図10に示すフローチャート中のステップS43で実行されるライセンス取得処理の詳細な手順をフローチャートの形式で示している。

#### 【0142】

クライアントAは、事前にライセンス・サーバAにアクセスして登録処理を行なうことにより、リーフID、DNK（デバイス・ノード・キー）、クライアントAの秘密鍵及び公開鍵のペア、ライセンス・サーバの公開鍵、及び公開鍵の証明書を含むサービス・データを取得している（前述及び図6を参照のこと）。

#### 【0143】

ここで、リーフIDは、クライアント毎に割り当てられた識別情報を表わし、DNKは、そのライセンスに対応するEKB（有効化ブロック）に含まれる暗号化されているコンテンツ・キー $K_c$ を復号するのに必要なデバイス・ノード・キーである。

#### 【0144】

まず、クライアントAは、ユーザのキーボードやマウスなどの入力装置の操作

を介して、更新するライセンスの指定情報、並びにユーザIDとパスワードを入力する（ステップS61, S62）。

#### 【0145】

次いで、クライアントAは、入力されたユーザIDとパスワード、ライセンス指定情報、並びにサービス・データに含まれるリーフIDを含むライセンス要求を、ライセンス・サーバBに送信する（ステップS63）。

#### 【0146】

ライセンス・サーバAは、ユーザIDとパスワード、並びにライセンス指定情報に基づいてライセンスを発行し、要求元のクライアントAに送信する。ライセンス・サーバAによるライセンスの提供処理の詳細については後述に譲る。

#### 【0147】

クライアントAは、ライセンス・サーバAからライセンスを受信することができた場合には（ステップS64）、ライセンス取得・管理部においてそのライセンスを記憶する（ステップS65）。

#### 【0148】

他方、ライセンス・サーバAからライセンスを受信することができない場合には（ステップS64）、所定のエラー処理を実行して（ステップS66）、本処理ルーチン全体を終了する。ここで言うエラー処理は、例えば、コンテンツを利用するためのライセンスが得られないので、コンテンツ再生処理部の起動を禁止する動作などが挙げられる。

#### 【0149】

以上のようにして、クライアントAは、コンテンツ・データに付随しているライセンスIDに対応するライセンスを取得して、初めてそのコンテンツを使用することが可能になる。

#### 【0150】

なお、図11に示すようなライセンス取得処理は、コンテンツのダウンロード後ではなく、その前に行なっておくことも可能である。

#### 【0151】

図12には、ライセンス・サーバからクライアントに提供されるライセンスの

データ構造を模式的に示している。同図に示すように、ライセンスは、使用条件、リーフIDやライセンス・サーバの電子署名などを含んでいる。

#### 【0152】

使用条件には、そのライセンスに基づいてコンテンツを使用することが可能な使用期限、そのライセンスに基づいてコンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいてコンテンツをコピーすることができる回数（許容されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいてコンテンツをCD-Rなどの記録媒体に記録することができる権利、可搬型の記録媒体にコピーすることができる回数、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログを取る義務などを示す情報などが含まれている。

#### 【0153】

図13には、クライアントA側からのライセンス要求（図11に示すフローチャート中のステップS63）に対応して実行される、ライセンス・サーバAがクライアントAにライセンスを提供するための処理手順をフローチャートの形式で示している。

#### 【0154】

ライセンス・サーバAは、クライアントAからアクセスを受けるまで待機する（ステップS71）。そして、クライアントAからアクセスを受けたときに、クライアントAに対して、ユーザIDとパスワード、並びにライセンスIDの送信を要求する。これに対し、クライアントAからは、ステップS63の処理として、ユーザIDとパスワード、リーフID並びにライセンス指定情報（ライセンスID）を送信するので、ライセンス・サーバA側ではこれらを取り込む（ステップS72）。

#### 【0155】

次いで、ライセンス・サーバAは、業務系データベース・サーバAに対して、ユーザIDとパスワードの照合処理を依頼し（ステップS73）、クライアントAの正当性をチェックする（ステップS74）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップS75）、本処理ルーチン全体を終

了する。この場合、クライアントAに対してライセンスは発行されない。

#### 【0156】

一方、照合処理が成功裏に終了した場合には、ライセンス・サーバAは、さらに課金サーバAにアクセスして、与信処理を依頼する（ステップS76）。課金サーバAは、ライセンス・サーバAからの与信処理の要求に応答して、そのユーザIDとパスワードに対応する過去の支払い履歴などを調査し、そのユーザが過去にライセンスの対価の不払いなど好ましくない実績があるかどうかをチェックする（ステップS77）。

#### 【0157】

ここで、好ましくない支払い実績があるなど与信が妥当でないと判断された場合には、課金サーバAは、ライセンス付与を不許可とする与信結果をライセンス・サーバAに返信する。ライセンス・サーバAは、これに応答して所定のエラー処理を実行して（ステップS78）、本処理ルーチン全体を終了する。この場合、クライアントAに対してライセンスは発行されない。

#### 【0158】

一方、与信OKであれば、次いで、ライセンス指定情報に対応するライセンスをライセンス蓄積部から取り出す（ステップS79）。ライセンス蓄積部に格納されているライセンスは、あらかじめライセンスID、バージョン、作成日時、有効期限などの情報が記述されている。

#### 【0159】

ライセンス・サーバAは、取り出したライセンスにリーフIDを付加する（ステップS80）。

#### 【0160】

次いで、ライセンス・サーバAは、このライセンスに対応付けられている使用条件を選択する（ステップS81）。あるいは、ライセンス要求時にユーザから使用条件が指定されている場合には、その使用条件が必要に応じてあらかじめ用意されている使用条件に付加される。そして、選択された使用条件をライセンスに付加する。

#### 【0161】

次いで、ライセンス・サーバAは、自身の秘密鍵によりライセンスに電子署名を施すことで、図12に示したようなライセンスを生成する（ステップS82）。そして、このライセンスを要求元のクライアントAに送信する（ステップS83）。

#### 【0162】

次いで、ライセンス・サーバAは、いま送信したライセンス（使用条件、リーフIDを含む）をユーザIDとパスワードに対応付けて記憶しておく。また、業務系データベース・サーバAにアクセスして、送信したライセンスのライセンスIDをユーザIDに対応付けて記録する（ステップS84）。業務系データベースAに記録した内容は、同期処理により業務系データベースCにも反映されており、他方の配信事業者Bからも利用することができる。

#### 【0163】

最後に、ライセンス・サーバAは、課金サーバAにアクセスして、ユーザIDとパスワードに対応するユーザに対する課金処理を実行する（ステップS85）。課金サーバAは、この課金処理の要求に応答して、該当するユーザに対する課金処理を実行する。課金サーバAは、クレジット・カードなどを用いた信用決済やデビット・カードを用いた即時決済、電子マネーによる支払い、現金払いや金融機関への振込みなどに対応してもよい。但し、課金処理の形態は本発明の要旨に直接関連しないので、本明細書ではこれ以上説明しない。

#### 【0164】

なお、課金処理に対してユーザが支払いを行なわなかったような場合には、そのユーザは与信を失い、以後ライセンスの付与を要求したとしてもライセンスを受けることができないことになる。すなわち、ユーザが与信を失った場合には、上述したように、課金サーバからライセンスの付与を不許可とする与信結果が返されるので、ライセンス・サーバはステップS78においてエラー処理を実行する。エラー処理では、例えば要求元のクライアントに対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了する。また、要求元のクライアントでは、ライセンスを受けることができないので、すなわちコンテンツを利用すること（暗号を復号すること）ができないことになる。

**【0165】**

図14には、図10に示すフローチャート中のステップS45において、クライアントが実行する、ライセンス・サーバに対するライセンスの更新処理の詳細な手順をフローチャートの形式で示している。

**【0166】**

まず、クライアントAは、ユーザのキーボードやマウスなどの入力装置の操作を介して、ライセンス指定情報、ユーザID、及びパスワードを入力する（ステップS91、S92）。

**【0167】**

次いで、クライアントAは、入力されたユーザIDとパスワード、並びにライセンス指定情報を含むライセンス更新要求を、ライセンス・サーバに送信する（ステップS93）。

**【0168】**

ライセンス・サーバA側では、ライセンス更新要求に応答して、使用条件を提示してくる（後述）。これに対し、クライアントAは、提示された使用条件を受信し、これをユーザに表示出力する（ステップS94）。

**【0169】**

ユーザは、キーボードやマウスなどの入力装置を操作して、画面表示されている使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。このようにして選択された使用条件（すなわちライセンスを更新する条件）を購入するための申し込みを、ライセンス・サーバAに送信する（ステップS95）。

**【0170】**

ライセンス・サーバA側では、クライアントAからの購入申し込みに応答して、最終的な使用条件を送信してくる（後述）。これに対し、クライアントAは、ライセンス・サーバAからの使用条件を受信して（ステップS96）、これを対応するライセンスの使用条件として更新する（ステップS97）。

**【0171】**

また、図15には、図10に示すフローチャート中のステップS45（図14

) に対応してライセンス・サーバで実行される、有効期限の切れたライセンスを更新するための詳細な処理手順をフローチャートの形式で示している。

#### 【0172】

ライセンス・サーバAは、クライアントAからのアクセスを受けると（ステップS101）、クライアントAが送信したライセンス更新要求（前述）を受信する（ステップS102）。

#### 【0173】

そして、ライセンス・サーバAは、更新要求されているライセンスに対応する使用条件（更新する使用条件）をライセンス蓄積部から読み出し、これを要求元のクライアントAに送信する（ステップS103）。

#### 【0174】

クライアントA側では、受信した使用条件をユーザに表示出力する。そして、ユーザは、キーボードやマウスなどの入力装置を操作して、画面表示されている使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。このようにして選択された使用条件（すなわちライセンスを更新する条件）を購入するための申し込みを、ライセンス・サーバAに送信する（前述）。

#### 【0175】

ライセンス・サーバAは、クライアントAからの使用条件の購入が申し込みされると、申し込まれた使用条件に対応するデータを生成し、クライアントAに送信する（ステップS104）。クライアントA側では、ライセンス・サーバAからの使用条件を受信して、これを対応するライセンスの使用条件として更新する（前述）。

#### 【0176】

ここで、クライアントが、ライセンス・サーバから供給されたライセンスに基づいて、コンテンツ・サーバから供給されたコンテンツを利用する処理の仕組みについて、図21を参照しながらまとめておく。

#### 【0177】

コンテンツ・サーバからクライアントに対してコンテンツが提供されるととも

に、ライセンス・サーバからクライアントにライセンスが供給される。コンテンツは、コンテンツ・キー  $K_c$  により暗号化されており ( $\text{Enc}(K_c, \text{Content})$ )、コンテンツ・キー  $K_c$  は、ルート・キー  $K_R$  ( $EKB$  から得られるキーであって、図 9 に示したコンテンツ・データ中のキー  $K_{EKB_C}$  に対応する) で暗号化され ( $\text{Enc}(K_R, K_c)$ )、 $EKB$ とともに、暗号化されてコンテンツに吹かされて要求元クライアントに提供される。

#### 【0178】

図 21 に示した例における  $EKB$  には、例えば図 22 に示すように、DNK で復号可能なルート・キー  $K_R$  が含まれている ( $\text{Enc}(DNK, KR)$ )。したがって、クライアントは、サービス・データに含まれる DNK を利用して、 $EKB$  からルート・キー  $K_R$  を得ることができる。さらに、ルート・キー  $K_R$  を用いて、 $\text{Enc}(KR, K_c)$  からコンテンツ・キー  $K_c$  を復号することができ、このコンテンツ・キー  $K_c$  を用いて、暗号化コンテンツ  $\text{Enc}(K_c, Content)$  からコンテンツを復号することができる。

#### 【0179】

##### 業務系データベース間の情報更新：

クライアント A とコンテンツ配信事業者 A の間でコンテンツやライセンスのダウンロードが行なわれると、その情報が配信事業者 A 内の業務系データベース A に記録される。本実施形態に係るコンテンツ配信システムでは、配信事業者 A 及び配信事業者 B 間での事業協力により同一顧客のクライアント A 及びクライアント B 間でのコンテンツの共有を実現するために、業務系データベース A の更新情報を業務系データベース C に反映させて、配信事業者 B からも利用可能にする。

#### 【0180】

配信事業者 A からクライアント A へ、コンテンツ又はライセンスのダウンロードが終了すると、業務系データベース A 及び C では、以下に示す各テーブルの該当するエントリーが更新される。

#### 【0181】

- (1) リーフ ID とクライアント ID の対応テーブル
- (2) クライアント ID とクライアントの公開鍵証明書の対応テーブル

- (3) クライアント ID とユーザ ID の対応テーブル
- (4) コンテンツ ID とライセンス ID の対応テーブル
- (5) ユーザ ID とダウンロードしたコンテンツのコンテンツ ID の対応テーブル（他にダウンロードした日時やライセンス ID なども記録することができる）
- (6) ユーザ ID とダウンロードしたライセンスのライセンス ID の対応テーブル（他にダウンロードした日時なども記録することができる）

#### 【0182】

##### コンテンツ・コピー証明書の発行：

この時点では、クライアント A は、移動するコンテンツを配信事業者から既に購入済み（又はライセンス取得済み）である。クライアント A にダウンロードしたコンテンツをクライアント B において利用するために、別クライアントへコンテンツをコピーする許可書に相当する「コンテンツ・コピー証明書」を取得する。

#### 【0183】

図 16 には、クライアント A がライセンス・サーバ A からコンテンツ・コピー証明書を取得するための処理手順をフローチャートの形式で示している。

#### 【0184】

ユーザがディスプレイ画面をキーボードやマウスなどの入力装置を介して操作することによって、コンテンツのコピー証明書の発行処理が起動される。これに応答して、ネットワーク・インターフェース 106 を介して、ライセンス・サーバ A へアクセスする（ステップ S111）。

#### 【0185】

ライセンス・サーバ A へアクセスした結果、クライアントのディスプレイ画面上には、コンテンツ選択画面（図示しない）が表示される。ユーザは、同画面上で、キーボードやマウスなどの入力装置を介して所望のコンテンツを指定するとともに、ライセンス ID、コピー先となるクライアント（この場合はクライアント B）のクライアント ID を入力する。そして、クライアント A は、コンテンツを指定する情報を、ライセンス ID と、コピー先のクライアント ID とともにライセンス・サーバ A へ通知する（ステップ S112）。さらに、ライセンス・サーバ A に対して、自己のユーザ ID 及びパスワードを通知する（ステップ S113）。

3)。

#### 【0186】

これに対し、ライセンス・サーバAは、コンテンツ・コピー証明書を発行して、これをクライアントAに返信する。そして、クライアントAは、送られてきたコンテンツ・コピー証明書を受信し（ステップS114）、これを一旦記憶する（ステップS115）。

#### 【0187】

また、図17には、ライセンス・サーバAがクライアントAからの要求に応答してコンテンツ・コピー証明書を発行するための処理手順をフローチャートの形式で示している。

#### 【0188】

ライセンス・サーバAは、クライアントAからアクセスを受けるまで待機する（ステップS121）。そして、クライアントAからアクセスを受けたときに、クライアントAに対して、コンテンツを指定する情報、ライセンスID、ユーザIDとパスワード、コピー先のクライアントIDの送信を要求する。これに対し、クライアントAからは、ステップS112及びS113の処理として、これらの情報を送信するので、ライセンス・サーバA側ではこれらを取り込む（ステップS122）。

#### 【0189】

次いで、ライセンス・サーバAは、業務系データベース・サーバAに対して、ユーザIDとパスワードの照合処理を依頼し（ステップS123）、クライアントAの正当性をチェックする（ステップS124）。ここで、照合に失敗した場合には、所定のエラー処理を実行して（ステップS125）、本処理ルーチン全体を終了する。この場合、クライアントAに対してコンテンツ・コピー証明書は発行されない。

#### 【0190】

一方、ステップS124の照合処理が成功裏に終了した場合には、さらに業務系データベース・サーバAに対して、クライアントAが指定されたコンテンツを既に購入済みか（ライセンスを取得済みか）どうか、照合処理を依頼し（ステッ

PS126)、クライアントAが当該コンテンツを購入済かどうかをチェックする(ステップS127)。ここで、照合に失敗した場合には、所定のエラー処理を実行して(ステップS128)、本処理ルーチン全体を終了する。この場合、クライアントAに対してコンテンツ・コピー証明書は発行されない。なお、ステップS127におけるエラー処理は、正当なライセンスを改めて取得する処理であってもよい。

### 【0191】

ステップS127の照合処理が成功裏に終了した場合、今度は業務系データベース・サーバCに対して、クライアントAのユーザが、ステップS122で受信したクライアントIDで示されるクライアントBを実際に所持しているかどうか、照合処理を依頼し(ステップS129)、同一ユーザがクライアントBを所持するかどうかをチェックする(ステップS130)。ここで、照合に失敗した場合には、所定のエラー処理を実行して(ステップS131)、本処理ルーチン全体を終了する。この場合、クライアントAに対してコンテンツ・コピー証明書は発行されない。なお、ステップS131におけるエラー処理は、クライアントBを改めて事前登録する処理であってもよい。

### 【0192】

ステップS130における照合処理が成功裏に終了した場合は、さらに、業務系データベース・サーバAに対して、コンテンツ・コピー証明書、すなわち要求元のクライアントAから当該コンテンツをクライアントBにコピーする許可書を発行してもよいかどうか、確認処理を依頼し(ステップS132)、コンテンツ・コピー証明書の発行の是非をチェックする(ステップS133)。ここで、確認処理に失敗した場合には、所定のエラー処理を実行して(ステップS134)、本処理ルーチン全体を終了する。この場合、クライアントAに対してコンテンツ・コピー証明書は発行されない。

### 【0193】

一方、ステップS133における確認処理が成功裏に終了した場合には、業務系データベース・サーバCにアクセスして、クライアントBのリーフIDを取得する(ステップS135)。次いで、ステップS122で取得したライセンスI

Dに対応したライセンス情報を取得する（ステップS136）。そして、取得したライセンス情報とクライアントBのリーフIDを基に、クライアントBが当該コンテンツを利用することを許可するライセンスを作成する（ステップS137）。作成されたライセンスの構造は、図12に示した通りである。

#### 【0194】

次いで、ライセンス・サーバAは、このライセンスに対して、ライセンス・サーバBの秘密鍵で電子署名を施す（ステップS138）。

#### 【0195】

次いで、ステップS122において取得した情報を用いて、コンテンツ・コピー証明書を作成し、これにライセンス・サーバBの秘密鍵を用いて電子署名を施す（ステップS139）。ライセンス・サーバA及びBは、互いの秘密鍵を所持している（前述）。

#### 【0196】

次いで、ライセンス・サーバA電子署名が施されたコンテンツ・コピー証明書を、要求元のクライアントAに送信する（ステップS140）。

#### 【0197】

そして、最後に、業務系データベース・サーバAにアクセスして、送信したコンテンツ・コピー証明書と対応するコンテンツID、ユーザID、コピー先となるクライアントBのリーフIDに対応付けて記録する（ステップS141）。業務系データベースAに記録した内容は、同期処理により業務系データベースCにも反映されており、他方の配信事業者Bからも利用することができる。

#### 【0198】

本実施形態では、コンテンツ・コピー証明書を取得時の代金は有料であっても無料であってもよい。また、有料の場合であっても、通常のライセンス取得時の料金に対して割り引いてもよい。これらの判断は、コンテンツ配信時業者側に委ねられ、課金サーバによって制御される。

#### 【0199】

コンテンツ・コピー証明書の発行を有料で行なう場合、例えばステップS139とステップS140の間に課金処理が挿入される。このときの課金処理につい

て以下に説明する。

#### 【0200】

ライセンス・サーバAは、課金サーバAにアクセスして、与信処理を依頼する。課金サーバAは、ライセンス・サーバAからの与信処理の要求に応答して、そのユーザIDとパスワードに対応する過去の支払い履歴などを調査し、そのユーザが過去にライセンスの対価の不払いなど好ましくない実績があるかどうかをチェックする。与信OKであれば、ユーザIDとパスワードに対応するユーザに対する課金処理を実行する。

#### 【0201】

他方、好ましくない支払い実績があるなど与信が妥当でないと判断された場合には、課金サーバAは、コンテンツ・コピー証明書の付与を不許可とする与信結果をライセンス・サーバAに返信する。ライセンス・サーバAは、これに応答して所定のエラー処理を実行して、本処理ルーチン全体を終了する。この場合、クライアントAに対してコンテンツ・コピー証明書は発行されない。

#### 【0202】

図18には、ライセンス・サーバにより発行されるコンテンツ・コピー証明書のデータ構造を模式的に示している。同図に示すように、コンテンツ・コピー証明書は、当該証明書の通し番号と、コピー対象となるコンテンツのコンテンツIDと、ライセンスと、電子署名などで構成される。

#### 【0203】

ライセンスは、コピー先となるクライアント（この場合はクライアントB）を登録するライセンス・サーバ（この場合はライセンス・サーバB）の秘密鍵で電子署名が施されている（前述）。

#### 【0204】

電子署名は、証明書の通し番号、コンテンツID、及びライセンスの3つの値に対し、ライセンス・サーバBの秘密鍵を用いて作成される。

#### 【0205】

ライセンス及び電子署名がライセンス・サーバBの秘密鍵で署名されていることから、コピー先のクライアントBは、ライセンス・サーバBの公開鍵を用いて

復号することができる。

#### 【0206】

##### コンテンツ及びコンテンツ・コピー証明書の記録媒体へのコピー：

クライアントAにダウンロードしたコンテンツを、クライアントBにおいて利用するために、コンテンツ・コピー証明書を附加してコンテンツを移動する。

#### 【0207】

図1に示す例では、クライアントAにおいて、ダウンロードしたコンテンツを可搬型の記録媒体にコピーして、これをクライアントBに装填することによってコンテンツの移動を行なう。

#### 【0208】

この場合、クライアントA側では、コンテンツ蓄積部からコンテンツを取り出して、これを記録媒体に書き込むという処理が行なわれる。また、クライアントB側では、記録媒体に記録されたコンテンツを読み出してコンテンツ蓄積部に格納するという処理が行なわれる。

#### 【0209】

勿論、ライセンスのないコンテンツを別のクライアントに移動する方法は、これに限定されるものではない。例えば、記録媒体以外に、有線・無線通信によってユーザ自らがクライアント間でのコンテンツのやりとりを行なってもよい。あるいは、一方のクライアントでコンテンツを購入すると、コンテンツ配信事業者が、同じユーザが保有する別のクライアントへも自動配信を行なうようにしてもよい。

#### 【0210】

図19には、クライアント間でコンテンツを移動する際の、移動元となるクライアントA側で行なう処理手順をフローチャートの形式で示している。

#### 【0211】

まず、移動対象となるコンテンツ・データをコンテンツ蓄積部から取り出して、記録媒体へコピーする（ステップS151）。

#### 【0212】

次いで、上述した処理手続きに従って取得したコンテンツ・コピー証明書を、

記録媒体へコピーする（ステップS152）。

【0213】

そして、クライアントA内のコンテンツ・コピー証明書を削除しておく（ステップS153）。

【0214】

なお、コンテンツ・コピー証明書の削除処理は、証明書の無断の複製や不正利用を防止するためであり、セキュリティ上問題がなければステップS153を省略することができる。

【0215】

コンテンツ取り込み処理：

クライアントB側では、クライアントA側でコンテンツ・データ並びにコンテンツ・コピー証明書がコピーされた記録媒体を装填して、内部に取り込むことにより、このコンテンツを利用することができる。

【0216】

図20には、コンテンツのコピー先であるクライアントB側でコンテンツを取り込むための処理手順をフローチャートの形式で示している。

【0217】

クライアントBでは、まず、装填した記録媒体からコンテンツ・データとコンテンツ・コピー証明書を取り込んで、記憶する（ステップS161）。

【0218】

次いで、コンテンツ・コピー証明書の電子署名を、ライセンス・サーバBの公開鍵を用いて検証し（ステップS162）、署名が正しいかどうか、すなわちコンテンツ・コピー証明書が改竄されていないかどうかをチェックする（ステップS163）。

【0219】

ここで、署名が正しくない、すなわちコンテンツ・コピー証明書が改竄されていると判断された場合には、ステップS163の分岐N0からステップS164に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、ク

ライアントB上ではコンテンツを利用できなくなる。

#### 【0220】

一方、署名が正しいと判断された場合には、次いで、コンテンツ・コピー証明書の通し番号を用いて、同一のコンテンツ・コピー証明書を既に使用したことがあるかどうかを検証し（ステップS165）、このコンテンツ・コピー証明書を用いた履歴の有無をチェックする（ステップS166）。

#### 【0221】

ここで、同じコンテンツ・コピー証明書を用いた履歴がある場合には、ステップS166の分岐N<sub>0</sub>からステップS167に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、クライアントB上ではコンテンツを利用できなくなる。

#### 【0222】

同じコンテンツ・コピー証明書を用いた履歴がない場合には、記録媒体より取り込んだコンテンツのコンテンツIDがコンテンツ・コピー証明書に記述されているコンテンツIDと一致するかどうかを検証し（ステップS168）、双方のコンテンツIDが一致するかどうかをチェックする（ステップS169）。

#### 【0223】

ここで、双方のコンテンツIDが一致しない場合には、ステップS169の分岐N<sub>0</sub>からステップS170に進み、所定のエラー処理を実行して本処理ルーチン全体を終了する。この場合、コンテンツ・コピー証明書からライセンスを取り出すことができないので、クライアントB上ではコンテンツを利用できなくなる。

#### 【0224】

双方のコンテンツIDが一致する場合には、コンテンツ・コピー証明書内のライセンスを取り出して、記憶する（ステップS171）。

#### 【0225】

そして、コンテンツのヘッダに、取り出したライセンスのライセンスIDを加え（ステップS172）、これをコンテンツ蓄積部に格納する。この結果、記録

媒体から取り出されたコンテンツ・データのコピーは、図9に示したものと同じ形式となるので、コンテンツ再生処理部は通常のコンテンツ再生処理（前述並びに図10を参照のこと）に従ってコンテンツを再生することができる。

#### 【0226】

そして、最後にコンテンツ・コピー証明書の通し番号を、「使用済みコンテンツ・コピー証明書」として、クライアントB内に記録する（ステップS173）。

#### 【0227】

なお、ステップS163, S166, S169に相当するコンテンツ・コピー証明書の正当性チェックのアルゴリズムについては、耐タンパ性のある処理として構成することが望ましい。

#### 【0228】

クライアントBでは、上述したような処理手順に従って取り込んだコンテンツ・データを図10に示したコンテンツ再生処理に従ってコンテンツを再生することができる。

#### 【0229】

まず、クライアントBは、ユーザがキーボードやマウスなどの入力装置の操作を介して指示したコンテンツの識別情報（C I D）を取得する（ステップS41）。コンテンツが指示されると、次いで、そのコンテンツに対応するライセンスI Dを読み取る。

#### 【0230】

次いで、読み取られたライセンスI Dに対応するライセンスが、クライアントにより既に取得され、ライセンス取得・管理部に保管されているかどうかを判断する（ステップS42）。

#### 【0231】

該当するライセンスが未だ取得されていない場合には、ステップS43に進み、ライセンス取得処理を実行する。但し、この時点では、コンテンツ・コピー証明書から取り出されたライセンスがライセンス取得・管理部に保管されているので、ライセンスが既に取得されていると判断される。

**【0232】**

次いで、このライセンスが有効期限内かどうかを判断する（ステップS44）。ライセンスの有効期限が既に満了していると判断された場合には、ステップS45に進み、ライセンスの更新処理を実行する。クライアントBは、図14に示す処理手順に従ってライセンス更新処理を行なう。

**【0233】**

ステップS44において、ライセンスが有効期限内であると判断された場合、あるいはステップS45においてライセンスが更新された場合、さらにライセンスが正当であるかどうかを判断する（ステップS46）。ライセンスが正当でない場合には、エラー処理を行なってから（ステップS47）、

**【0234】**

ステップS46において、ライセンスが正当であると判断された場合、該当する暗号化コンテンツ・データをコンテンツ蓄積部から読み出す（ステップS48）。そして、暗号化されているコンテンツ・データを、図9に示したデータに配置されている暗号化ブロック単位で、コンテンツ・キー $K_c$ を用いて復号する（ステップS49）。

**【0235】**

さらに、復号されたコンテンツ・データをデコードし、コンテンツの再生処理を行なう（ステップS50）。

**【0236】****[追補]**

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

**【0237】****【発明の効果】**

以上詳記したように、本発明によれば、コンテンツの不正利用を防止しながら

、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用するこ<sup>ト</sup>とを可能にすることができる、優れたコンテンツ配信システム、コンテンツを利用する情報処理装置又は情報処理方法、並びにコンピュータ・プログラムを提供することができる。

#### 【0238】

本発明によれば、それぞれのコンテンツ配信事業者と接続可能な別々のクライアントにて購入したコンテンツを各クライアントで共有して使用することができる。但し、別のクライアントで利用する際、それが有料又は無料のいずれであるかはコンテンツ配信事業者や著作権保有者などの独自の判断で設定することができる。

#### 【0239】

また、本発明によれば、一方のクライアントで購入したコンテンツを別のクライアントと共有して利用するために課金が発生する場合には、その別のクライアントを使用するだけで課金処理を行なうことができるので、顧客の利便性が向上する。

#### 【0240】

また、本発明によれば、一方のクライアントで設定又は更新した再生環境情報（再生リスト、再生設定（音量設定、連続再生設定など）、G U I 画面、購入予定楽曲へのブックマークなど）を、他方のクライアントにおいても繁栄させることができる。

#### 【図面の簡単な説明】

##### 【図 1】

本発明の一実施形態に係るコンテンツ配信システムの構成例を模式的に示した図である。

##### 【図 2】

各種サーバあるいはクライアントとして動作するホスト装置のハードウェア構成を模式的に示した図である。

##### 【図 3】

ホストがクライアントとして動作するときの機能構成を模式的に示した図であ

る。

#### 【図 4】

ホストがライセンス・サーバとして動作するときの機能構成を模式的に示した図である。

#### 【図 5】

ホストがコンテンツ・サーバとして動作するときの機能構成を模式的に示した図である。

#### 【図 6】

クライアントがライセンス・サーバに事前登録を行なうための処理手順を示したフローチャートである。

#### 【図 7】

コンテンツをダウンロードする際のクライアント側の処理手順を示したフローチャートである。

#### 【図 8】

コンテンツをダウンロードする際のコンテンツ・サーバ側の処理手順を示したフローチャートである。

#### 【図 9】

コンテンツ・サーバAからクライアントAにコンテンツを配信するときに用いられるデータ・フォーマットの構成例を示した図である。

#### 【図 10】

クライアントA側でダウンロードしたコンテンツを再生するための処理手順を示したフローチャートである。

#### 【図 11】

クライアントA側でダウンロードしたコンテンツを再生するために必要なライセンスを取得する処理手順を示したフローチャートである。

#### 【図 12】

ライセンス・サーバからクライアントに提供されるライセンスのデータ構造を模式的に示した図である。

#### 【図 13】

ライセンス・サーバAがクライアントAにライセンスを提供するための処理手順を示したフローチャートである。

【図14】

クライアントが実行する、ライセンス・サーバに対するライセンスの更新処理の詳細な手順を示したフローチャートである。

【図15】

ライセンス・サーバによるライセンスを更新するための詳細な処理手順を示したフローチャートである。

【図16】

クライアントAがライセンス・サーバAからコンテンツ・コピー証明書を取得するための処理手順を示したフローチャートである。

【図17】

ライセンス・サーバAがクライアントAからの要求に応答してコンテンツ・コピー証明書を発行するための処理手順を示したフローチャートである。

【図18】

コンテンツ・コピー証明書のデータ構造を模式的に示した図である。

【図19】

クライアント間でコンテンツを移動する際の、移動元となるクライアントA側で行なう処理手順を示したフローチャートである。

【図20】

コンテンツのコピー先であるクライアントB側でコンテンツを取り込むための処理手順を示したフローチャートである。

【図21】

クライアントが、ライセンス・サーバから供給されたライセンスに基づいて、コンテンツ・サーバから供給されたコンテンツを利用する処理の仕組みを説明するための図である。

【図22】

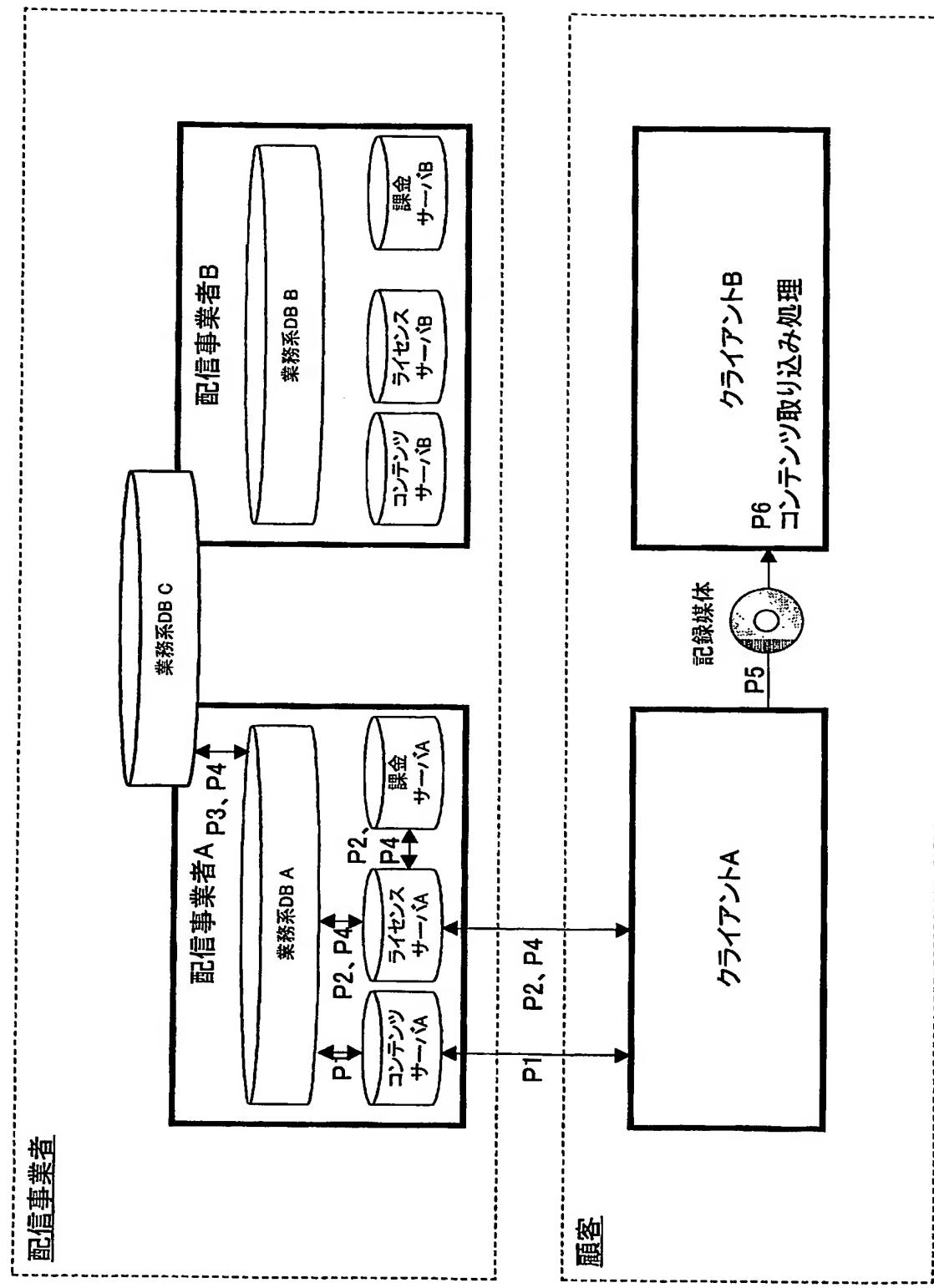
EKBの構造を示した図である。

【符号の説明】

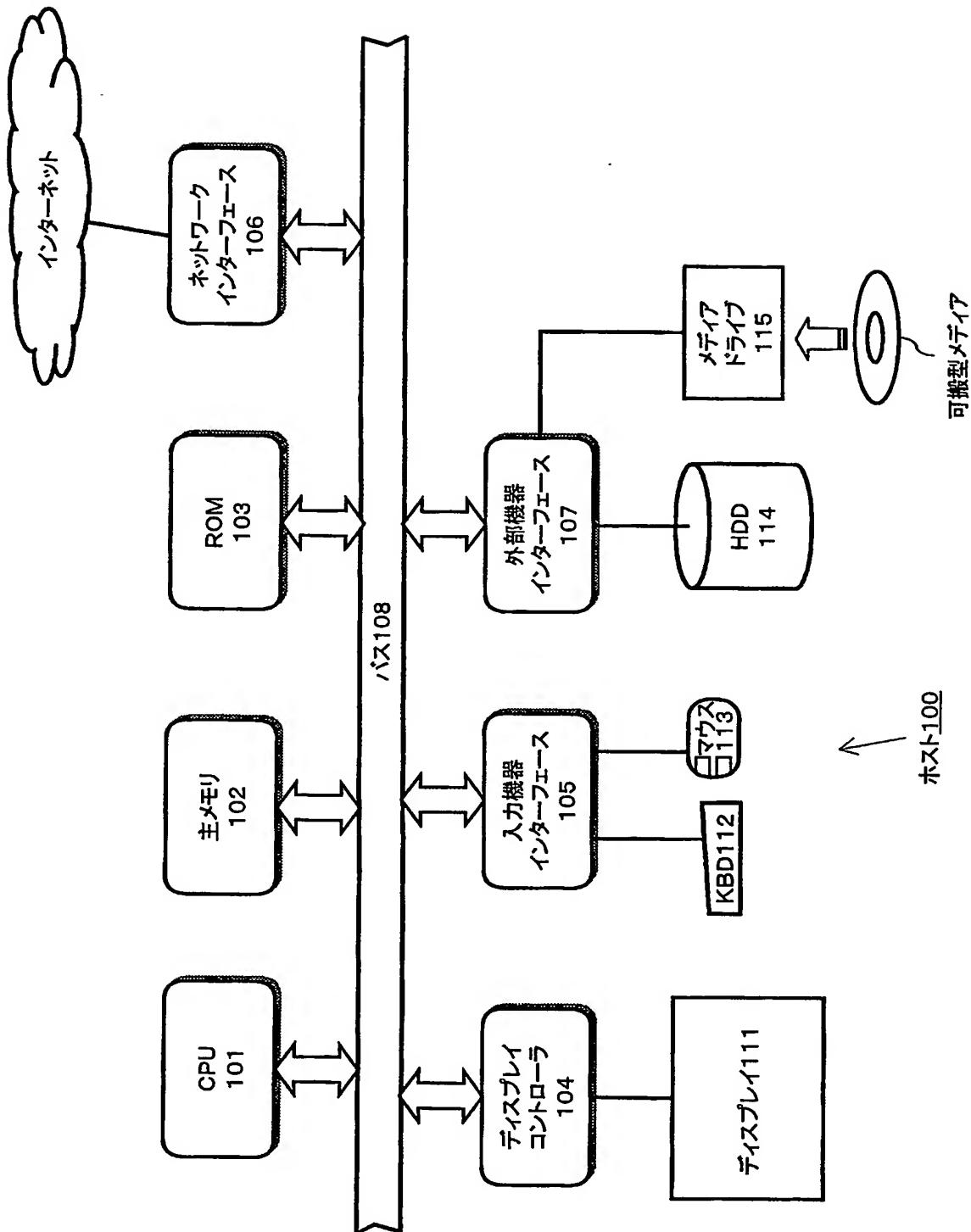
100…ホスト  
101…CPU,  
102…主メモリ, 103…ROM  
104…ディスプレイ・コントローラ  
105…入力機器インターフェース  
106…ネットワーク・インターフェース  
107…外部機器インターフェース  
108…バス  
111…ディスプレイ  
112…キーボード, 113…マウス  
114…ハード・ディスク装置  
115…メディア・ドライブ

【書類名】 図面

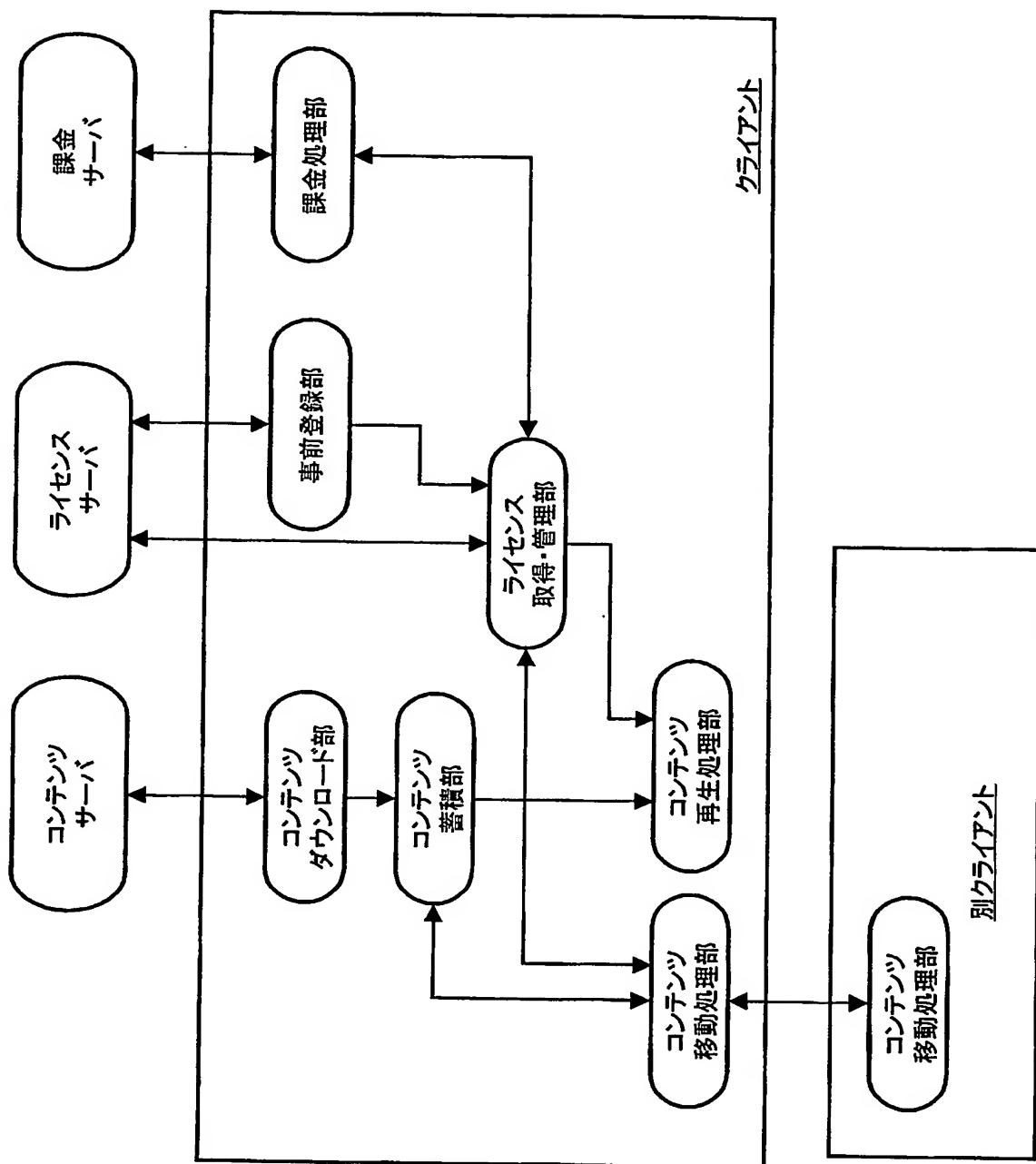
【図 1】



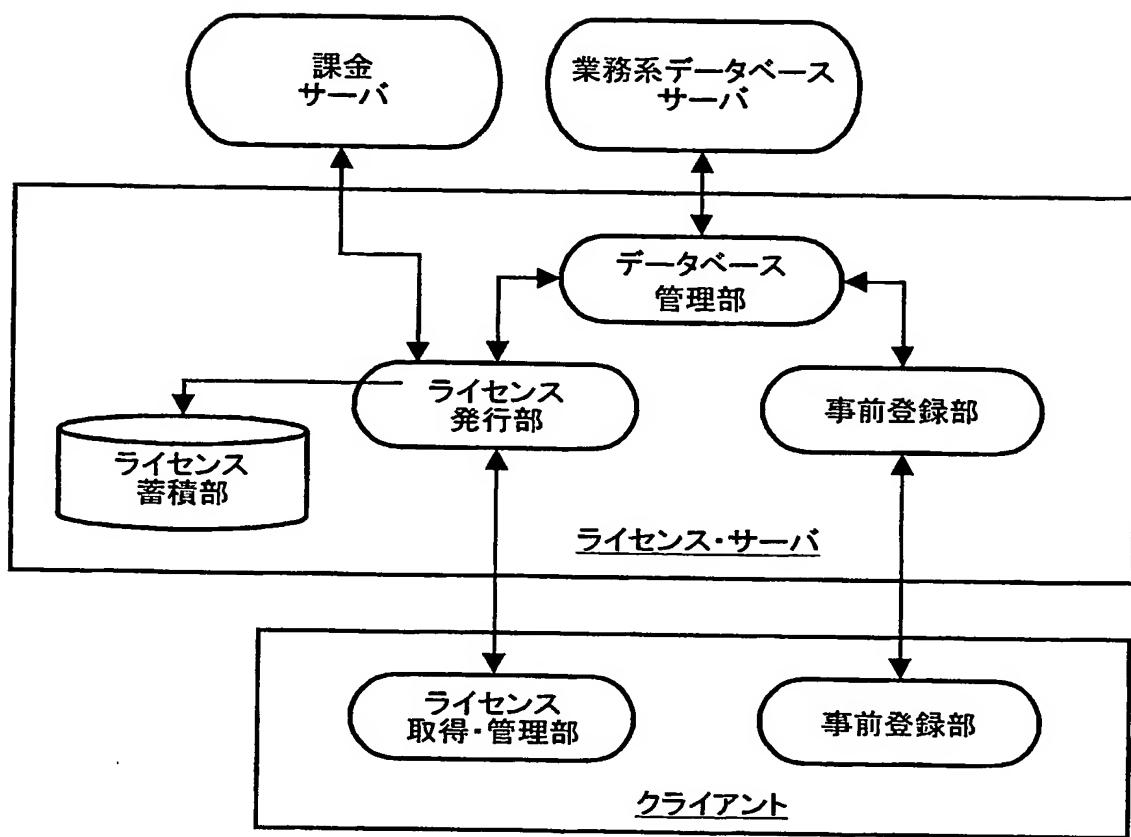
【図2】



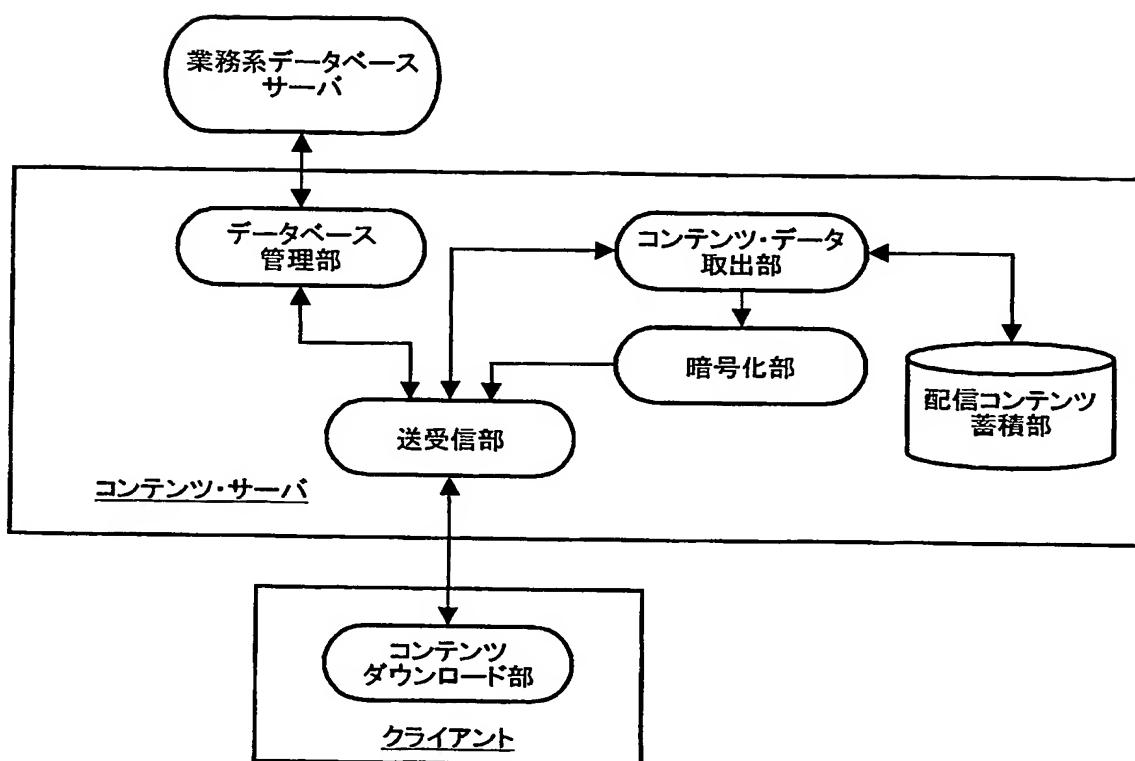
【図3】



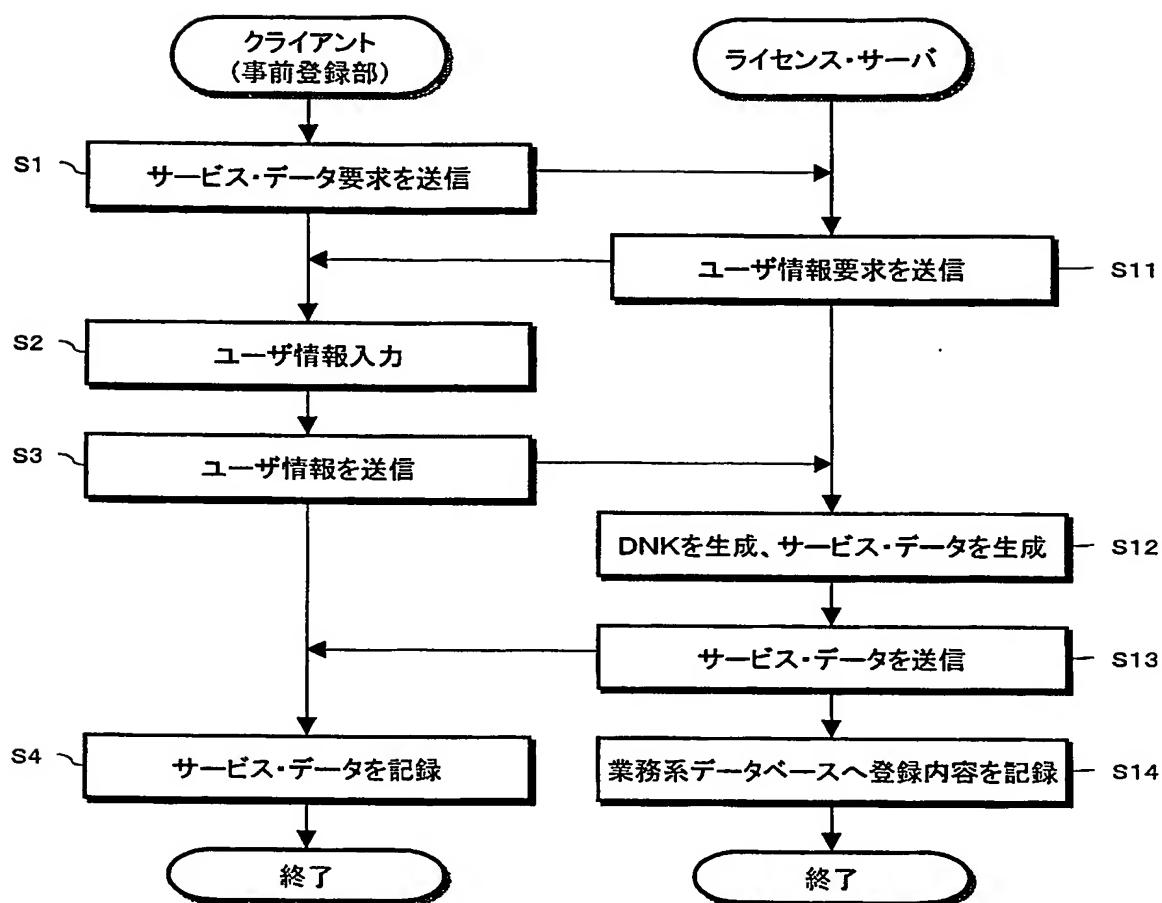
【図4】



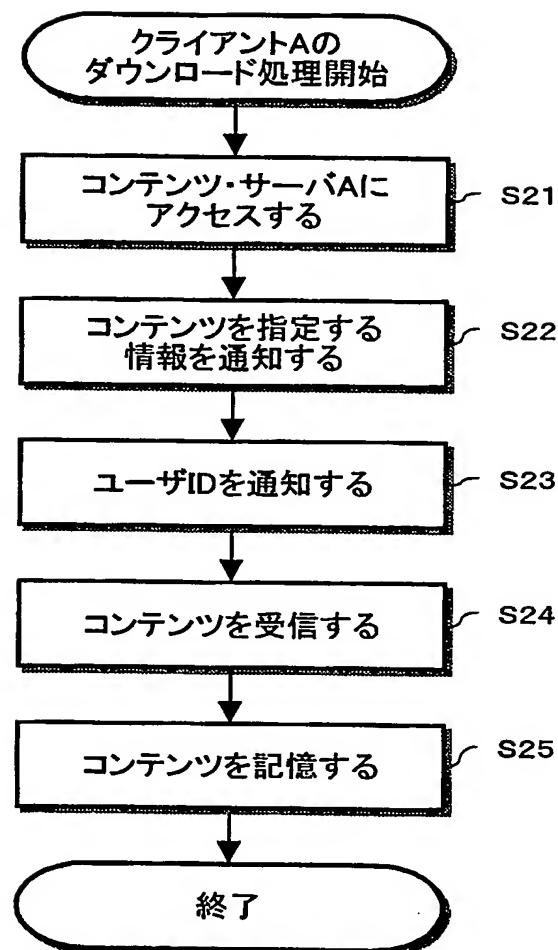
【図5】



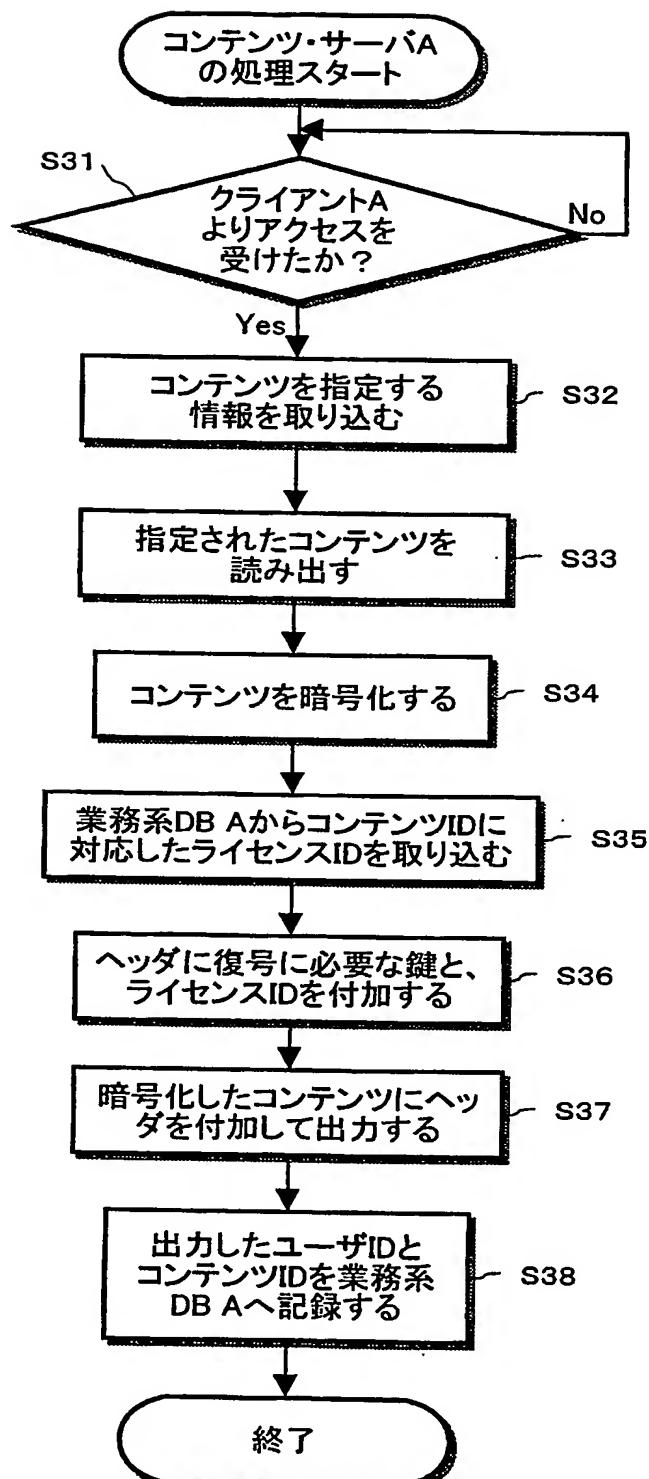
【図 6】



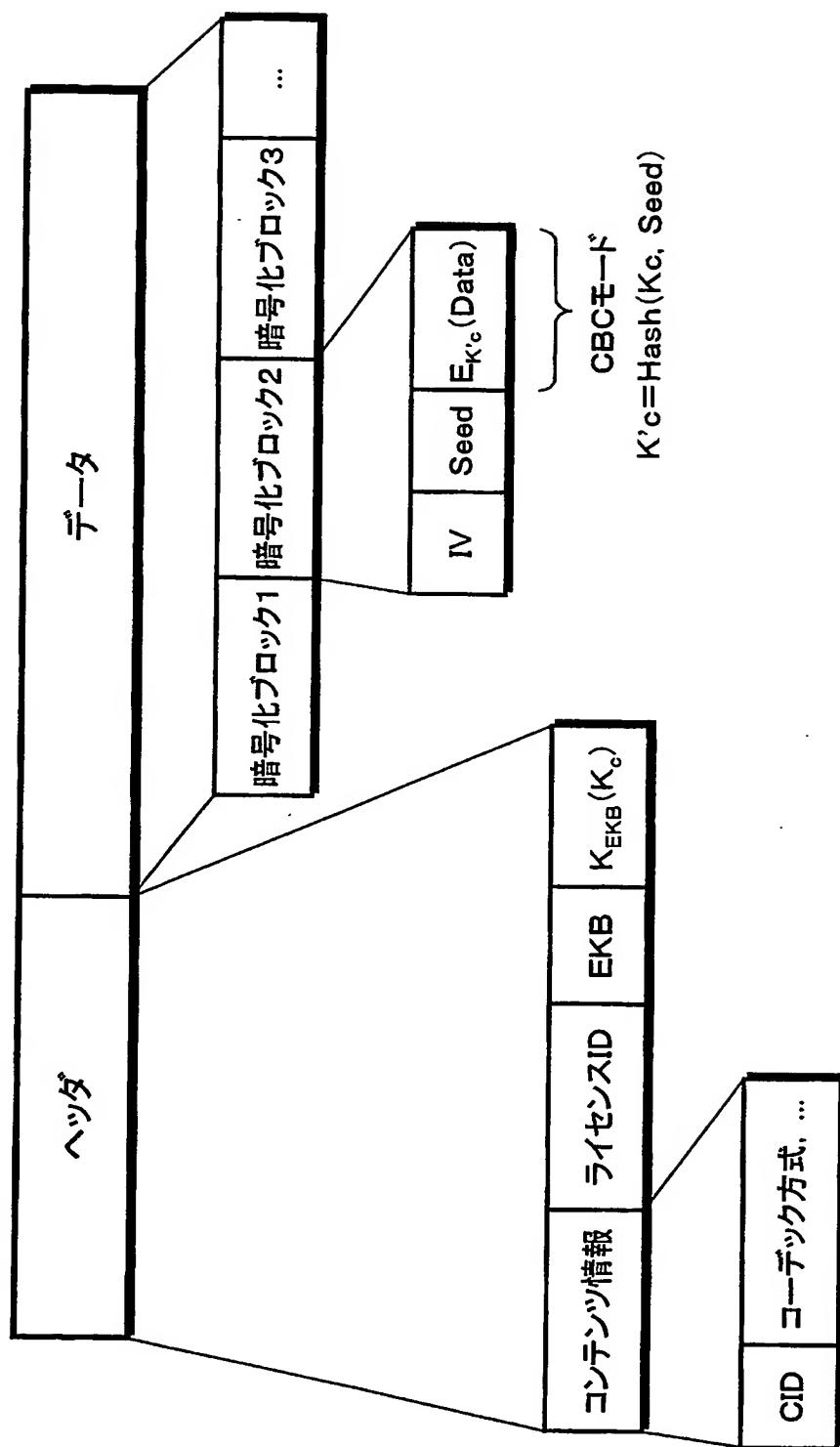
【図7】



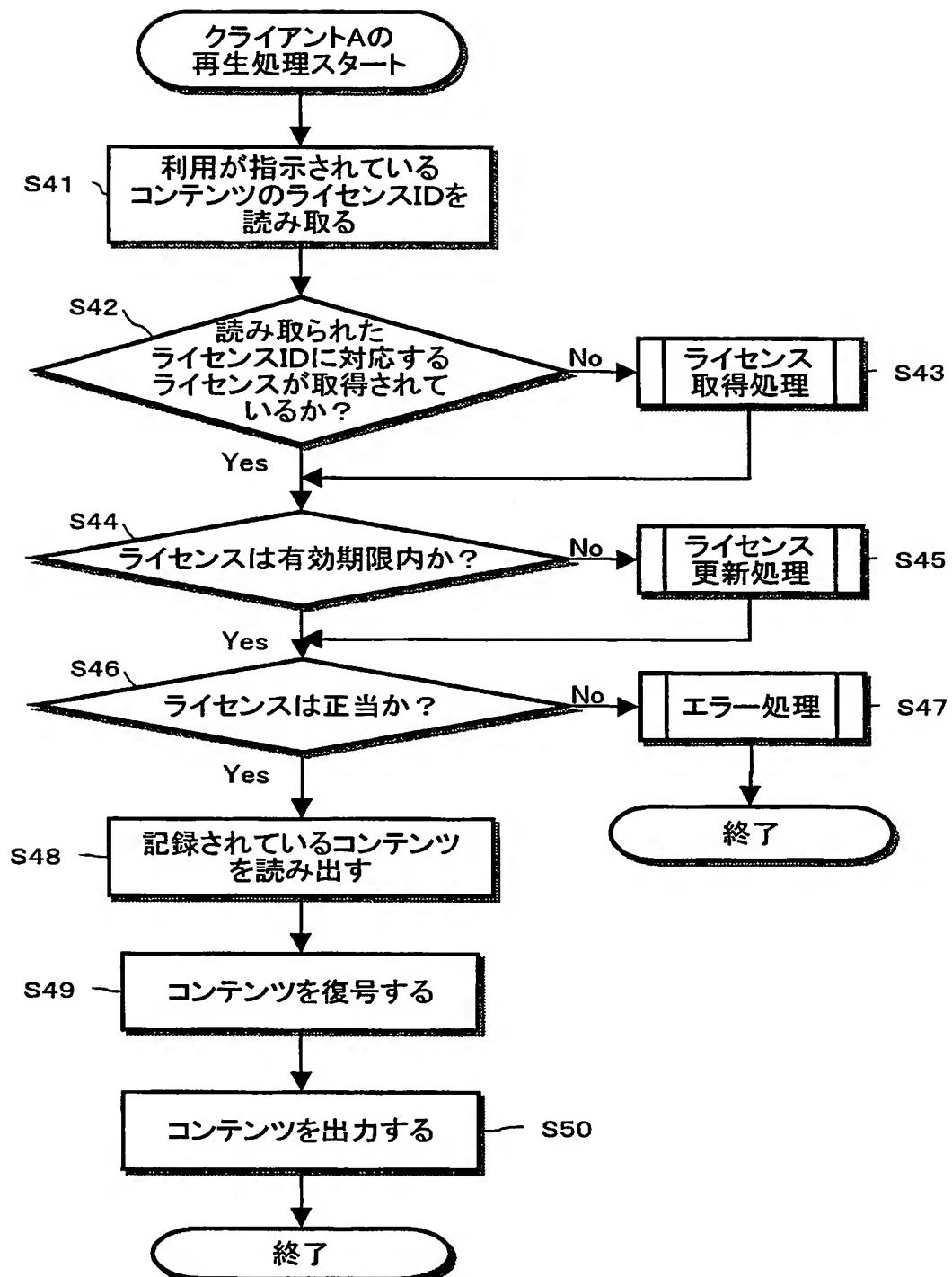
【図8】



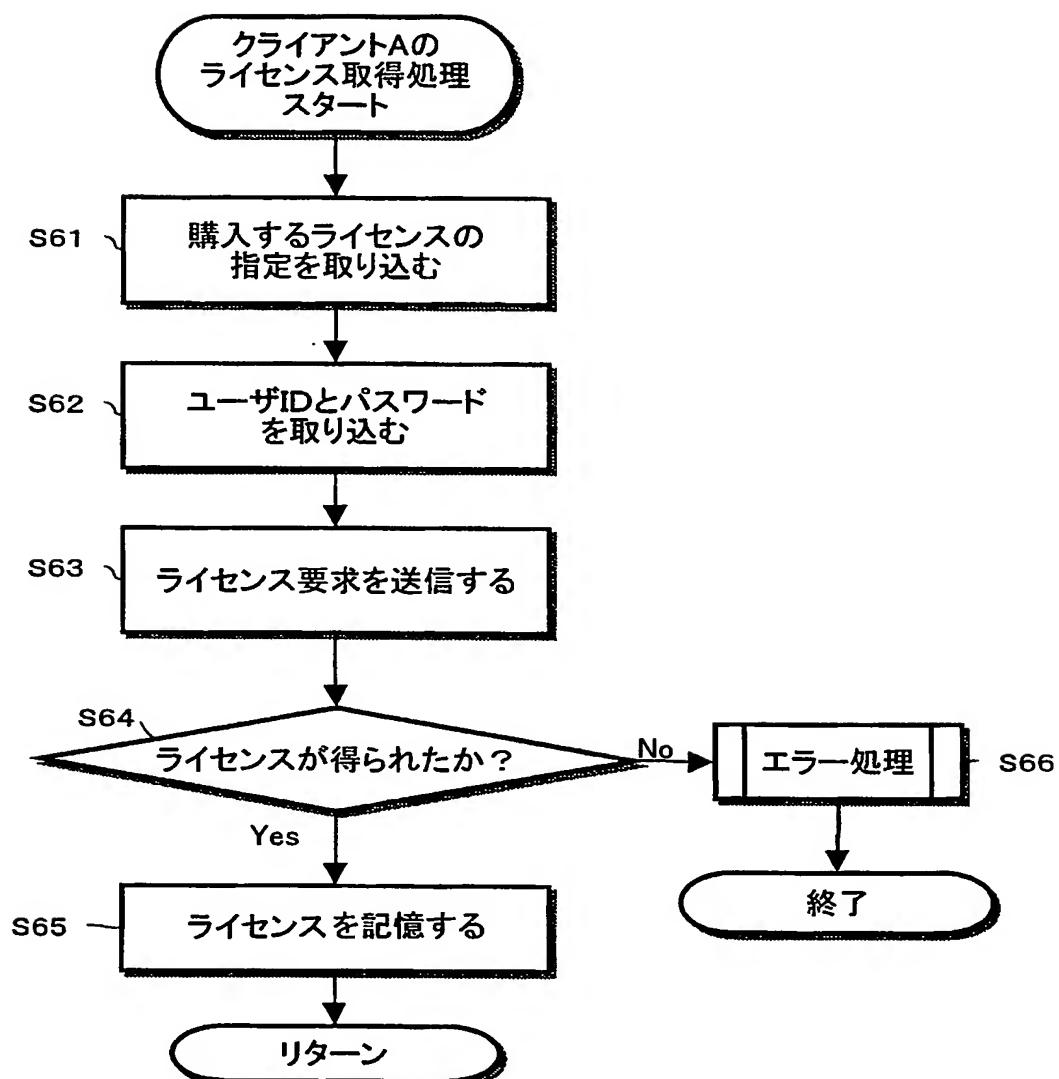
【図9】



【図10】



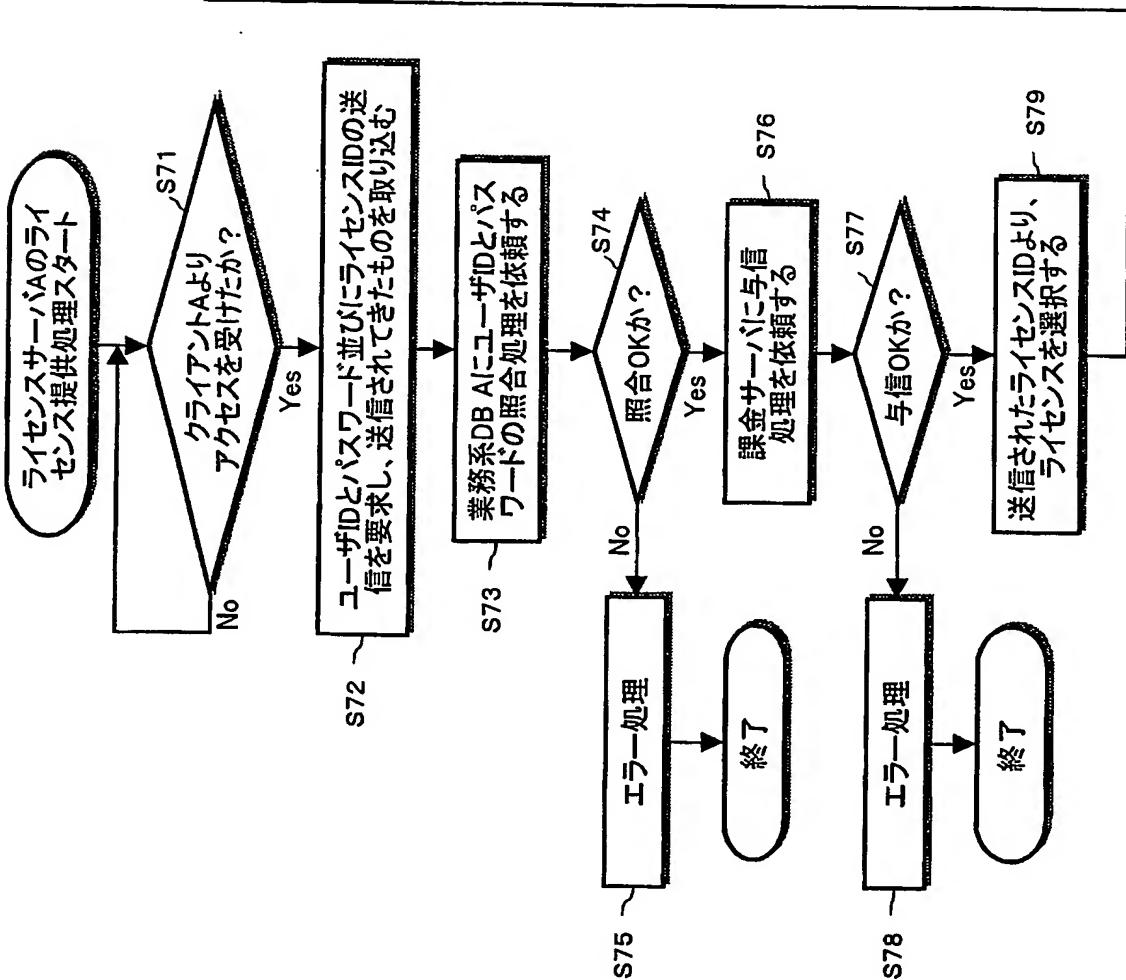
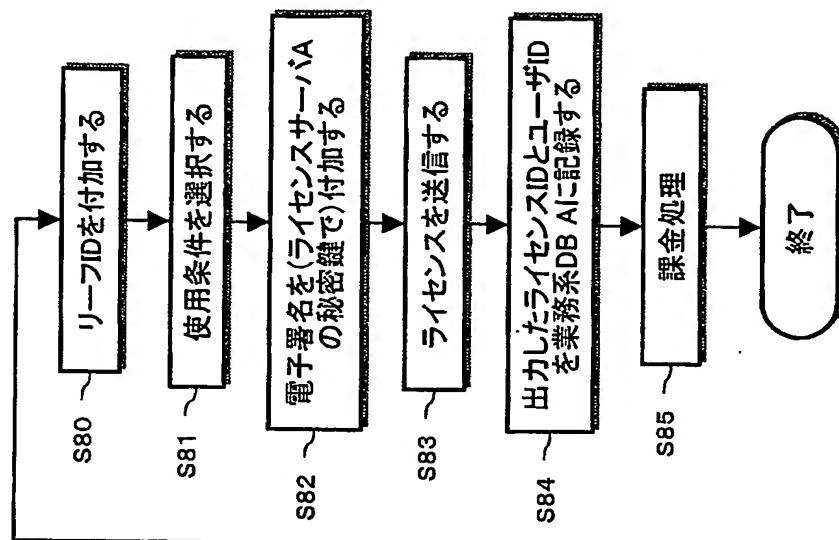
【図11】



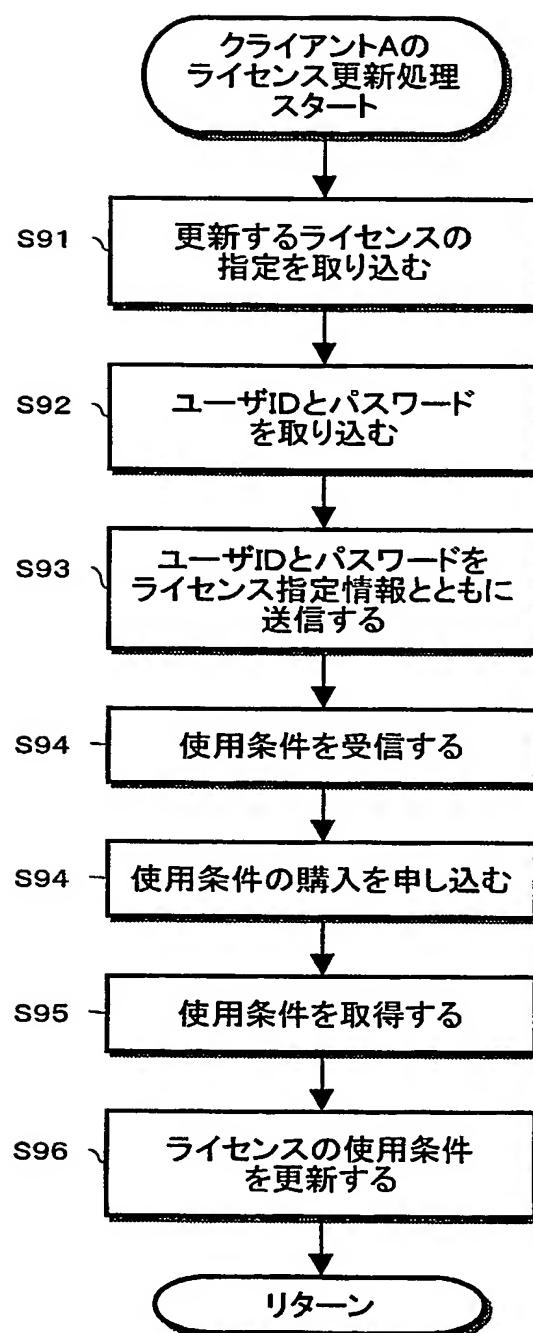
【図12】

ライセンスID
作成日時
有効期限
使用条件
リーフID
電子署名
ライセンス

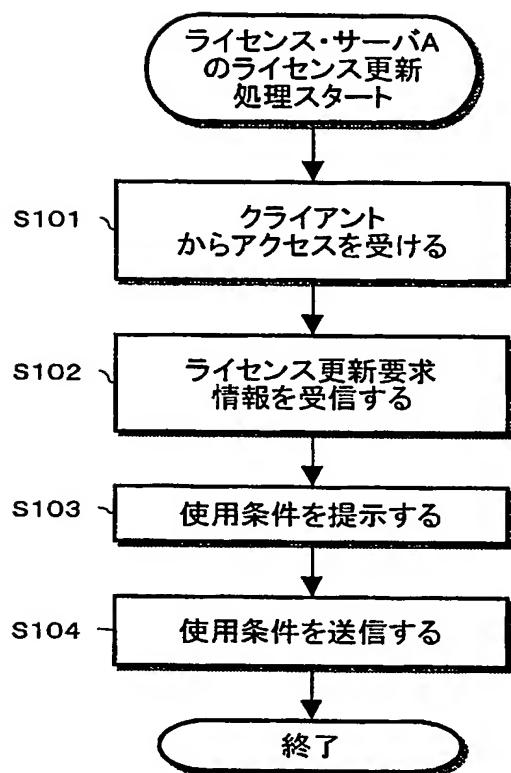
【図13】



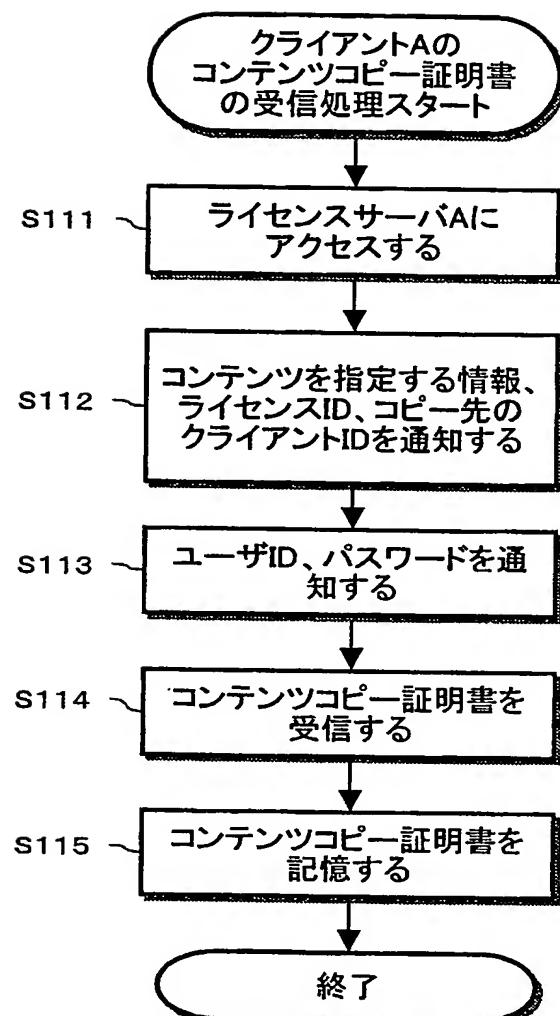
【図14】



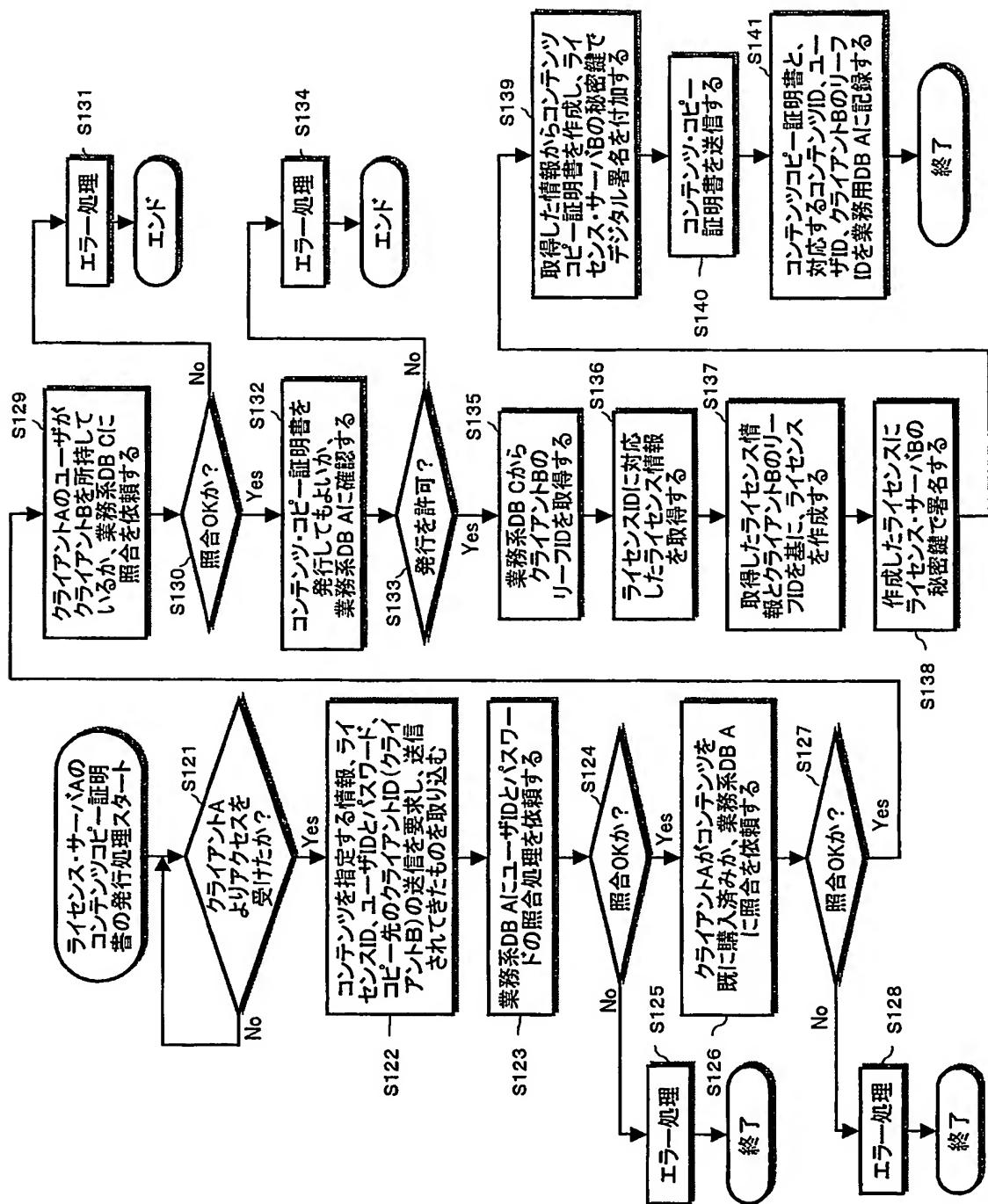
【図15】



【図16】



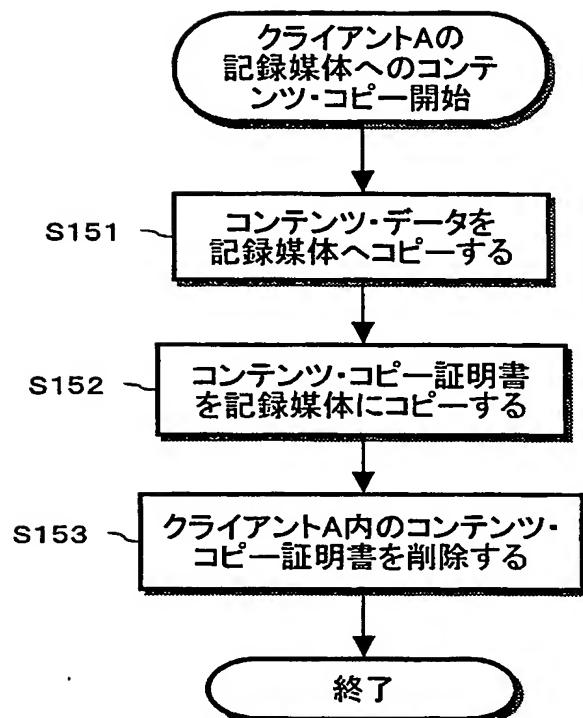
【図 17】



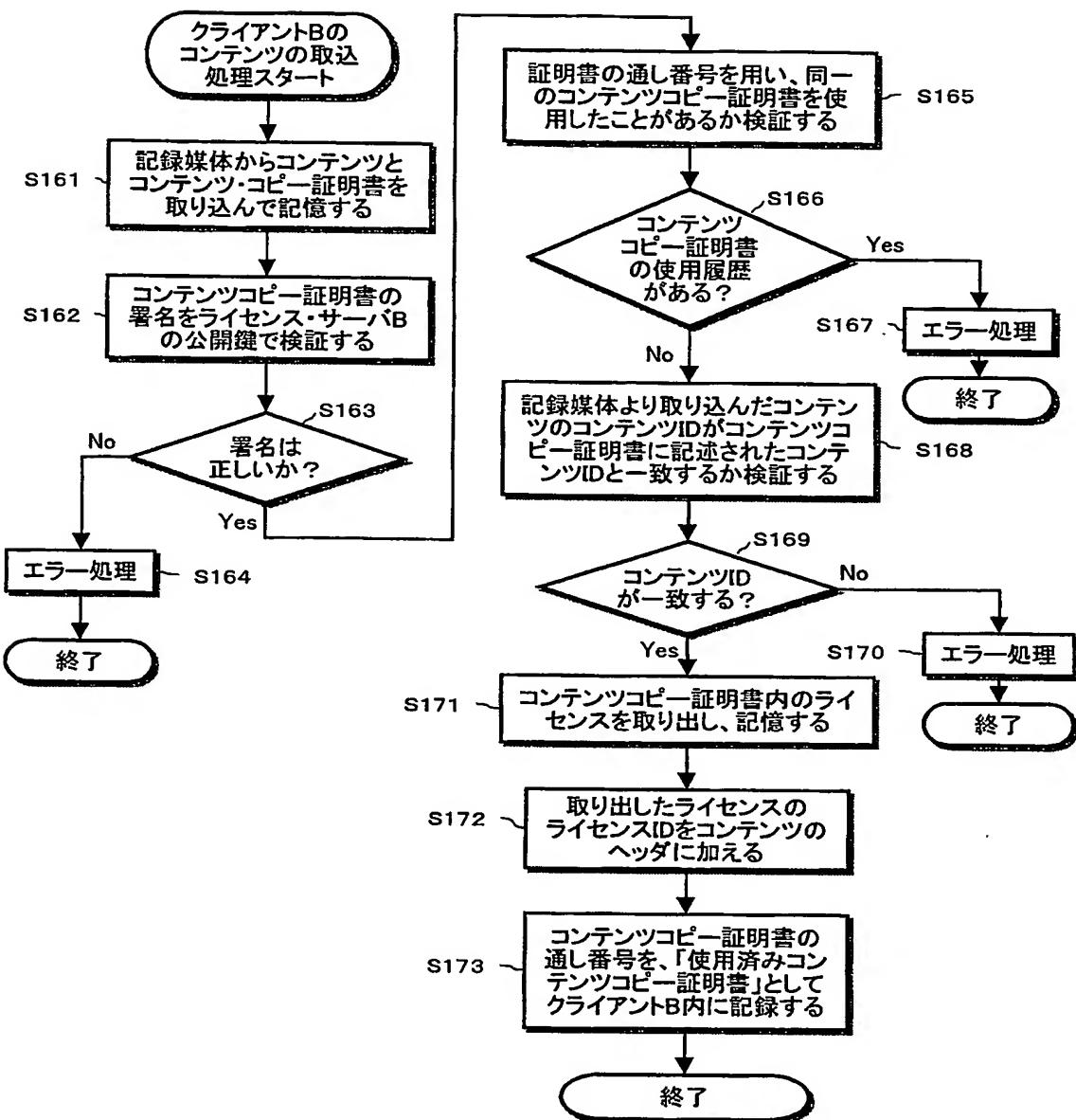
【図18】

証明書の通し番号
コピーするコンテンツのコンテンツID
ライセンス 〔ライセンスサーバAで作成 ライセンスサーバBの秘密鍵で署名〕
デジタル署名 (上記3つの値にライセンスサーバBの秘密鍵で署名)
コンテンツ・コピー証明書

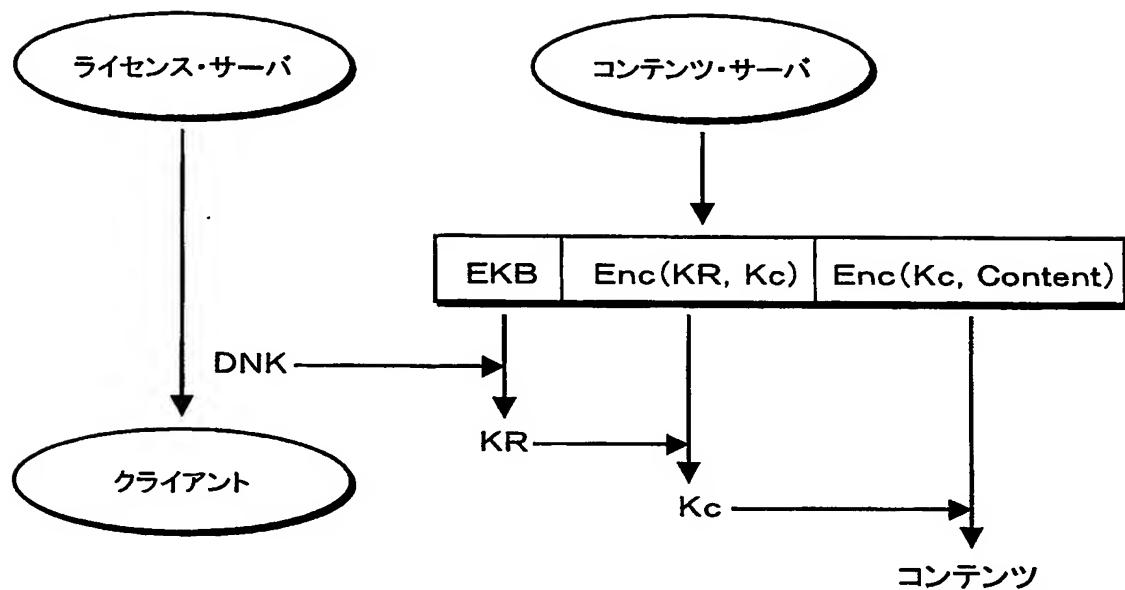
【図19】



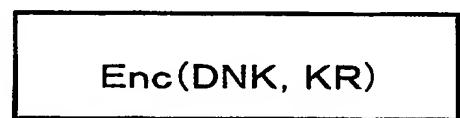
【図20】



【図 2 1】



【図 2 2】



【書類名】 要約書

【要約】

【課題】 コンテンツの不正利用を防止しながら、一旦ライセンスを受けた利用者が複数の機器に跨ってコンテンツを利用することを可能にする。

【解決手段】 著作権管理されている環境が提供され、暗号化されたコンテンツと、その暗号を解くライセンスを別物で扱うことができる。また、各クライアントは正当にコンテンツを使用する。クライアントAで取得したコンテンツをクライアントBに保管する際に、クライアントBの情報をそのコンテンツに付加し、クライアントBを特定できるようにすることにより、コンテンツの保護を担保しながらクライアントA及びB間でのコンテンツの共有を実現する。

【選択図】 図1

特願 2003-014245

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住所 東京都品川区北品川6丁目7番35号  
氏名 ソニー株式会社